PRV

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

PATENT- OCH REGISTRERINGSVERKET • PATENT- AND REGISTRATION OFFICE

(71) *Sökande* / *Applicant (s)* — *Telefonaktiebolaget L M Ericsson (publ), Stockholm SE*

(21) *Patentansökningsnummer* / *Patent application number* — *0203297-7*

(86) *Ingivningsdatum* / *Date of filing* — *2002-11-05*

Stockholm, 2003-04-04

För Patent- och registreringsverket
For the Patent- and Registration Office

Lina Oljeqvist

Avgift
Fee

PATENT- OCH REGISTRERINGSVERKET
SWEDEN

Postadress/Adress
Box 5055
S-102 42 STOCKHOLM

Telefon/Phone
+46 8 782 25 00
Vx 08-782 25 00

Telex
17978
PATOREG S

Telefax
+46 8 666 02 86
08-666 02 86

REMOTE SERVICE EXECUTION IN AN HETEROGENEOUS NETWORK ENVIRONMENT

FIELD OF THE INVENTION

[0001] The present invention generally relates to the inter-working and compatibility between services offered by the core network and applications residing at the service network. In particular, the invention relates to the development of an open standard interface between the core network and the service network.

BACKGROUND

[0002] Today, big players in the telecommunication market have several types of access and core networks technologies distributed along the countries were they operate for providing the users with access to telecom networks and to Internet. Exemplary technologies of the types above commented, such as GPRS, EDGE, CDMA, TDMA, D-AMPS, PDC, CDMA-2000, WCDMA, etc., as well as combinations thereof, derive in different scenarios where different heterogeneous environments turn up. Thus, apart from the complexity introduced by such heterogeneous environments, the administrative divisions among these networks into several local small companies adds more heterogeneity to the environment and makes more complex the provision of unified services and service application accesses to users roaming through different core networks.

[0003] New competitors can be added now to these big players that used to operate networks out of the traditional telecom premises. These new competitors

nowadays are a part of the telecommunications market, specially in all issues related to data transmission, while allowing roaming, wider broadband access than conventional PLMN networks, and adding other value added services to users. These companies may operate several types of networks as well, such as small WLAN local operators, Satellite operators, cable operators, etc.

[0004] In such a market scenario for telecommunication network, old and new network operators have its own customer base, and therefore the efforts to develop applications and services are more complex than before due to the great diversity of technology and administrative environments.

[0005] The interaction and compatibility among service layers in such heterogeneous environments have to be solved in order to provide a user with a true Virtual Home Environment (VHE) for allowing users to have access to a same application, as well as for allowing applications to have access to users and services, independently of the access and core networks where such users are presently roaming. In this respect, Service Network Roaming (hereinafter referred to as SNR) and Remote Services Execution (hereinafter referred to as RSE) appear as key factors for allowing the users to have a true Virtual Home Environment (VHE).

[0006] One exemplary instance of the efforts made nowadays to standardize an Open Service Access (OSA) interface between the service network layer and the core network layer is the OSA/PARLAY standardization group. This group is working on the development of an open standard interface between the core network and the service network based on a number of Application Programming Interfaces (APIs). These

APIs allow developers to access the services offered by the core network in an easy way.

[0007] These Application Programming Interfaces (APIs) were initially defined within the so-called Parlay group, and standardized under 3rd Generation Partnership Project (3GPP) and European Telecommunication Standard Institute (ETSI) standardization bodies. In this context, the service network concept along with the above APIs are traditionally referred to as "Parlay" within the Parlay group whereas 3GPP and ETSI usually refer them as "Open Service Access" (OSA). For the sake of clarity, the term OSA/PARLAY is currently used throughout this instant specification for referring the interface layer between the core and the service networks.

[0008] Thus, OSA/PARLAY allows users and developers to access and to offer applications using services offered by the operator's core home network. The original aim was that the above APIs would be network independent, thus enabling the evolution of core networks technologies without impacts on the applications.

[0009] Therefore, a conventional architecture based on OSA/PARLAY comprises Applications that are formally included in a service network and deployed on Application Servers (AS), a number of Service Capability Features (SCF) representing interface classes of the OSA/PARLAY interface and implemented in Service Capability Servers (SCS), an OSA/PARLAY Framework (OSA-FW) for providing framework capabilities to applications such as a controlled access to the Service Capability Features, and core network elements. In particular, the Applications running on Application Servers (AS) use the Service Capability Features provided by the Service Capability Servers (SCS), and thus the SCS implements the server side of the API whereas the AS

implements the client side. The SCS may interact with core network elements such as the Home Location Register (HLR), Mobile Switching Center (MSC), Call Status Control Function (CSCF), etc.

[0010] Applications/Clients access OSA/PARLAY functions in terms of service capability features via a standardized application interface. This means that service capability features are accessible and visible to application/clients via the method/operation invocations in the OSA/PARLAY API interface. More specifically and under a 3GPP environment, OSA/PARLAY allows Applications access to Home network Service Capability Features.

[0011] The above OSA/PARLAY functions have been generally grouped on three different types to distinguish:

- Framework functions, for providing commonly used utilities, necessary for access control, security, resilience and management of OSA/PARLAY functions;
- Network functions, for enabling the applications to make use of the functionality of the underlying network capabilities; and
- User data related functions, for enabling applications to access data of a particular user, such as the status of the user, location, or data in a corresponding user Profile.

[0012] In particular, the Framework provides the essential capabilities that allow OSA/PARLAY applications to make use of the service capabilities in the Home network, and more specifically Security Management including Authentication and Authorization, Service Registration and Discovery functions, and Integrity Management.

[0013] Regarding the methods/operations in the OSA/PARLAY API interface commented above, three types of interface classes have been distinguished:

- interface classes between the Applications in the service network and the Framework for providing the applications with basic mechanisms, like Authentication for instance, that enable said Applications to make use of the service capabilities in the home network of a user;

- interface classes between Applications and Service Capability Features (SCF), which are individual services that may be required by the client to enable the running of third party applications over the interface, like Messaging type service for instance; and

- interface classes between the Framework and the Service Capability Features, which provide the mechanisms necessary for supporting a multi-vendor environment.

[0014] Nowadays, however, there is no way to run the execution of an application in a user's home network that makes use of network services from an heterogeneous visited network through the OSA/PARLAY interface. An exemplary use case may be an international healthcare company "X" wanting to track its heart patients not only through the wide area covered by PLMN networks but also within indoor spaces, like airports for example, using the coming Bluetooth positioning technology, or through transport facilities in a local underground network without coverage from a PLMN network but with a WLAN coverage. The WLAN may be located in the same or in a different country than the Home PLMN (HPLMN), provided that the HPLMN and the WLAN operators have an agreement of the type Service Level Agreement generally known under a Service Network environment. The

healthcare client application has no knowledge about the network where the patient's mobile terminal is when asking for such patient localization, but this functionality is a key for this healthcare company in order to monitor its patients, namely customers, as well as for receiving their respective hearth device alarms. Today this and other similar problems have not been solved yet for scenarios including a variety of networks because, even though these networks support an OSA/Parlay interface, this interface only works on top of the home core network.

[0015] Moreover, at the presently launching market scenario wherein big traditional operators are added new comer competitors, thus resulting in a great diversity of technology and administrative environments, the OSA/PARLAY architectural model commented above is variably distributed among different players in such manners that different administrative and business domains turn up.

[0016] Certain operators are organized in such a way that there is an organization responsible for the core network as well as for in-house developed end-user services and applications whereas another separate organization is responsible for providing end-user services through partners as well as for offering service capabilities to said partners. Such above different organizations imply somewhat different telecommunication domains that need to independently enforce their own policies and to gather their own service information. Thus, both domains instanced above would respectively get advantage of offering service capabilities from the other domain in addition to those offered by each domain itself, and this has been recently known in certain fora as a "Federation". In other words, different organizations, even different corporate firms, might get additional advantages of having a flexible

solution where a second domain can offer service capabilities, namely a Donor Domain, toward a first domain, namely a Receiver Domain, that in turn can offer these said capabilities to its own partners, namely its own service providers.

[0017] However, the architectural and interfacing model that OSA/PARLAY has focused on does not provide for a first domain offering its service capabilities to a second domain and vice versa, and neither does it where any of these domains has its own partners for offering the corresponding applications Service Level Agreements, namely policies, that may be enforced during a run-time service execution.

[0018] In this respect, an object of the present invention is to provide means an methods for enabling the execution of an application in a user's home network that makes use of network services from an heterogeneous visited network through the OSA/PARLAY interface.

[0019] Another object of the present invention is to enable a number of domains respectively offering service capabilities from the other domain in addition to those offered by each domain itself.

SUMMARY OF THE INVENTION

[0020] The above objects, among others, are accomplished in accordance with the invention by the provision of a telecommunication system and a method for providing ….

[0021] The telecommunication system supporting ….

[0022] A method is also provided by the present invention for providing ….

[0023] The method comprising the steps of:

– ...

– ...

– ...; and

– ... .

[0024] In particular, ...

[0025] ....

BRIEF DESCRIPTION OF DRAWINGS

[0026] The features, objects and advantages of the invention will become apparent by reading this description in conjunction with the accompanying drawings, in which:

[0027] **FIG. 1** illustrates a basic overview of ....

[0028] **FIG. 2** represents a system architecture comprising ....

[0029] **FIG. 3** presents a simplified flow sequence ....

[0030] **Fig. 4** shows the flow sequence that follows after having ....

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0031] In accordance with a first aspect of the present invention, there is provided a number of currently preferred embodiments of a system and method for supporting the execution of a service application in a user's home network that makes use of network services from an heterogeneous visited network through an extended and improved OSA/PARLAY interface.

[0032] Generally speaking and accordingly with a second aspect of the present invention, there is also provided a number of currently preferred embodiments of said system and method for allowing a first network domain, namely a donor domain, to offer its own service capabilities toward a second domain, namely a receiver domain, that in turn can offer these service capabilities to its own partners or service providers.

[0033] There are provided as well particular embodiments in accordance with a third aspect of the present invention, which is shared by the above two previous aspects, to allow the capture of agreements between different networks and domains and having these agreements enforced on run-time.

[0034] A basic architecture overview is shown in Fig. 2 to illustrate …

[0035] …

[0036] For the sake of clarity, the preferred or suitable embodiments can be better described ….

[0037] Different use cases are described following this for some of the above ….

[0038] A first use case to show in the above ….

[0039] Still another use case is the ….

[0040] …

[0041] The invention is described above in respect of several embodiments in an illustrative and non-restrictive manner. Obviously, many modifications and variations of the present invention are possible in light of the above teachings. The scope of the invention is determined by the claims, and any modification of the embodiments that fall

within the scope of these claims is intended to be included therein.

CLAIMS

1. A telecommunications system arranged for providing client service applications with access to service capability features via a standardized OSA/PARLAY interface (API), the system comprising a number of application servers (AS) where client service applications run, a number of service capability servers (SCS) where service capability features (SCF) are specified in a first network domain, a first logical Framework entity for providing a controlled access to said service capability features, and a number of core network elements, the telecommunications system **characterized in that** said first logical Framework entity is arranged for communicating with at least one second logical Framework entity for accessing service capability features (SCF) specified in a second network domain.

2. The telecommunications system of claim 1, wherein the first network domain is the Home core network of a user whereas the second network domain is a visited core network where the user is roaming.

3. The telecommunications system of claims 1 or 2, wherein
   -

   - ...;

   - ...;

   - ...; and

   - ... .

4. The telecommunications system of claim 3, ...

5. A method of providing client service applications with access to service capability features via a standardized interface (OSA/PARLAY API), the method comprising the steps of:

(a) registering service capability features in a first network domain with a first logical Framework entity;

(b) carrying out security management mechanisms for *authentication and authorization of* a number of players selected from a group that includes user, network, a requester application, and combinations thereof, through said first logical Framework entity;

(c) discovering service capability features that are available for use in said first network domain by the requester application;

the method **characterized by** including the steps of

(d) determining in the first network domain that service capability features at a second network domain are available for the requester application;

(e) carrying out security management mechanisms *for authentication and authorization* from a first logical Framework entity of said first network domain, through a second logical Framework entity of a second network domain; and

(f) discovering service capability features that are available for use in said second network domain by said requester application.

6. The method of claim 5, wherein the step of determining that service capability features are available at a

second network domain includes the step of requesting to the first logical Framework entity in the first network domain access to the service capability features available in the second network domain for the requester application.

7. The method of claim 6, wherein the step of determining that service capability features are available at a second network domain includes the step of receiving such indication from a service capability feature selected in the first network domain as a result of the previous step c).

8. The method of claim 5, wherein the step of discovering available service capability features in the second network domain comprises the step of negotiating capabilities from the first logical Framework entity of the first network domain with a service capability feature selected from those service capability features available for use in said second network domain by said requester application.

9. The method of claim 8, wherein the step of negotiating capabilities includes the step of creating an instance of said selected service capability feature at said second logical Framework entity, and the step of returning back to the requester application a reference to such instance.

10. The method of claim 5, further comprising the step of registering a second logical Framework entity of a second network domain in a first logical Framework entity of a first network domain.

11. The method of claim 10, further comprising the step of publishing at least one interface that allows said first and said second logical Framework entities to

access the service capability features respectively controlled by each other.

12. The method of claim 5, further comprising the step of exchanging information between a first and a second logical Framework entity about available service capability features in a first and a second network domain respectively, with or without explicit indication of the interface required to access such service capability features.

13. The method of claim 12, further comprising the steps of indicating to at least one service capability feature in a first network domain the service capability features available in a second network domain, and vice versa.

14. The method of any of claims 5 to 13, further comprising the step of capturing Service Level Agreements between the network operator of a network domain and a service provider of a requester application.

15. The method of claim 14, further comprising the step of capturing Service Level Agreements between a first and a second network domains through corresponding first and second logical Framework entities.

16. The method of claim 15, wherein said Service Level Agreements are extended between Donor Domains and Receiver Domains in a telecommunication network with multiple domains, the method further comprising the steps of:

- creating and assigning a Federation Service Profile on a Donor Framework;

- signing a Federation Service Agreement on a Donor Framework;

- installing (registering) a Donor Service in a Receiver Framework;

- requesting a Receiver Application Service Agreement from a Donor Framework.

17. The method of claim 16, wherein a Receiver Application Service Agreement serves as a partition of a Federation Service Agreement.

18. The method of any of claims 5 to 17, wherein the steps of carrying out security management mechanisms include the steps of handing out and handing over an Assertion that gives a practitioner the right to use a service in a federated framework setup.

19. The method of claim 18, further comprising the steps of:

- handing over an Assertion by a Receiver Framework to any other entity;

- signing an Agreement about the hand-out and or hand-over of an Assertion;

- requesting an Assertion; and

- a Donor enabler /SCS checking the validity of a received Assertion with a Donor Framework.

20. The method of any of claims 5 to 19, wherein each domain is operated by a different operator.

21. A method of constructing an ad hoc Proxy based on the information when a Service Enabler registers to a Donor Framework, the method comprising:

- downloading a Proxy from a Donor Domain; and
- allowing an operator of a Donor Domain to register an SCS as Proxy to a Receiver Domain.

22. The method of claim 18, wherein the information comprises service type and or supported property values.

ABSTRACT OF THE INVENTION

The invention provides a system and a method, basically oriented to the ….

+46 8 7520937

INVENTION DISCLOSURE 1 (16)

Uppgjord (även fakta ansvarig om annan) - *Prepared (also subject responsible if other)*	Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz	EEM/TD/R-02:062		
Dokansv/Godk - *Doc respons/Approved* / Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán			

Copy:
<inventors>

Receivers:
EEM Patent Support Office

Ink. t. Patent- och reg.verket
2002 -11- 05
Huvudfaxen Kassan

Invention Disclosure: Remote Service Execution in an heterogeneous network Environment

Responsible Patent Support Person: EEM/TD/R Tomas Iglesias Diaz

Project with which the work was performed:
Project sponsor/owner:

Would a patent be standard blocking?: YES
Where?
When?

Urgency of Filing: <provide a disclosure date>
Why?

EEM Number: **EEM02026**

Read and Understood by: ..... Date:.....

Read and Understood by: ..... Date:.....

Uppgjord (även fältansvarig om annan) - *Prepared (also subject responsible if other)*	Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz	EEM/TD/R-02:062		
Dokansv/Godk - *Doc respons/Approved* / Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán			

1 TECHNICAL INFORMATION

1.1 Name of invention

Remote Service Execution in an heterogeneous network environment.

1.2 Inventor(s)

Name :Alejandro Bascuñana Muñoz
Department : EEM/TD/R
Employee no. :3832
Phone no. :4400
e-mail/memo :Alejandro.Bascunana-Munoz@ece.ericsson.se
Account no. :12001

Omitance

1.3 Background

1.3.1 Abbreviations

API Application Programming Interface
APP Application
CAMEL Customised Application for Mobile Network Enhanced Logic
CSE Camel Service Environment
FW Framework
LFW Local Framework
RFW Remote Framework
HE Home Environment
HE-VASP Home Environment Value Added Service Provider
HLR Home Location Register
INAP Intelligent Networks Application Part
MAP Mobile Application Part
MT Mobile Terminal
MS Mobile Station
MSC Mobile Switching Centre
OSA Open Service Access
PLMN Public Land Mobile Network
PSE Personal Service Environment
SAT SIM Application Tool-Kit
SCF Service Capability Feature
SCP Service Control Point
SCS Service Capability Server
SIM Subscriber Identity Module
SNR Service Network Roaming
RSE Remote Service Execution
SMS Short Message Service
SMTP Simple Mail Transfer Protocol

Uppgjord (även ladsansvarig om annan) - Prepared (also subject responsible if other)	Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz	EEM/TD/R-02:062		
Dokansv/Godk - Doc respons/Approved / Kontr - Checked	Datum - Date	Rev	File
EEM/TD/R Julio López Roldán			

USIM User Service Identity Module
VASP Value Added Service Provider
VHE Virtual Home Environment
VLR Visited Location Register
VSCF Visited Service Capability Feature

1.3.2 General

Today big players in the wireless telephony market have several types of access and core networks technologies distributed along the countries were they operates, such as GPRS[i], EDGE[ii], CDMA[iii], TDMA,D-AMPS[iv], PDC[v], CDMA-2000[vi], WCDMA[vii], etc. just to provide to the users with access to telecom networks and to Internet. Besides the complexity introduced by such heterogeneous environment the administrative divisions among these networks into several local small companies adds more etherogeneity to the environment and makes more complex to provide roam users with unified services and application access. To those big players, now it can be added a new set of new competitors that used to operate networks out of the traditional telephonic networks, but now they are going to be a part of the telecommunications infrastructure specially in all issues related to data transmission, allowing roaming, wider broadband access than PLMN networks and adding other value added services to users. These companies operate several types of networks such are: small WLAN local operators, Satellite operators, cable operators, etc.
In this market network old and new network operators have its own customer base, and therefore the efforts to develop application and service are more complex than before due to the great diversity of technology and administrative environments.

The interaction and compatibility among their service layers it is something that should be reached in the future in order to provide to the user with a real VHE allowing the users to have access to the same application or to the applications to have access to their users independent of the access or core network where they are located, hold the same user profile, etc. Service Network Roaming (SNR) and Remote Services Execution (RSE) appears as one of the key factors that will allow to the users to have a real VHE.

Thanks to standards like CAMEL some service network roaming and remote services execution can be offered to the PLMN users, and some type of interaction it is allowed among telecom networks

One example of the effort done by the standardisation groups to standardise the interface between the service and the core network layer is the OSA/PARLAY[1] standardisation group. This group is working on the development of an open standard interface between the core network and the service network based on APIs. These APIs allow developers the access to the services offered by the core network in an easy way. There are several groups co-ordinating their efforts with

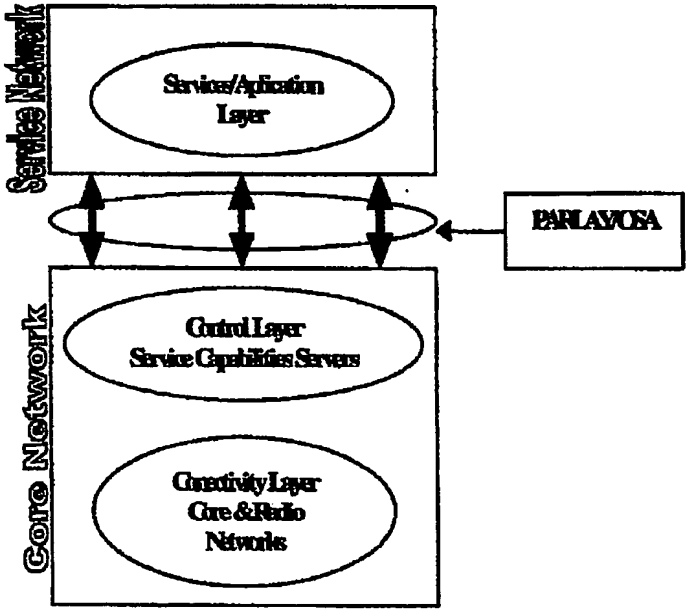
[1] http://www.parlay.org ; http://www.3gpp.org

Upprjord (även faktaansvarig om annan) - *Prepared (also subject responsible if other)*		Nr - *No.*	
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062	
Dokansv/Godk - *Doc respons/Approved*	Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán				

the OSA/PARLAY group, these standardisation groups are OSA/PARLAY, 3GPP, ETSI, ITU-T and JAIN.

OSA/PARLAY allows to users and to developers, to access and to offer applications using services offered by the operator's core network.
Due to the importance of network integration, the main goal of this work is related to the definition of a framework interface to allow the service roaming and the remote service execution among heterogeneous networks of the same or different network operators. The main standardisation model followed and improved will be the OSA/PARLAY.

This figure illustrates the layer distribution in an OSA/PARLAY environment.

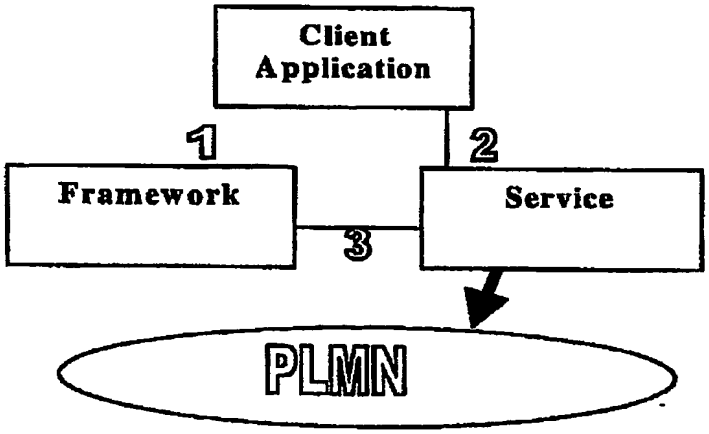


1.4 State-of-the-art

The OSA specifications define an architecture that enables to the service and application to make use of network functionality through an open standardized interface, i.e. the OSA/PARLAY API's. The network functionality is described as Service Capability Features (SCFs) or Services. The OSA Framework is a general component in support of Services (Service Capabilities) and Applications.The OSA API is split into three types of interface classes.

Uppgjord (även fakdansvarig om annan) - Prepared (also subject responsible if other)		Nr - No.	
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062	
Dokansv/Godk - Doc respons/Approved	Kontr - Checked	Datum - Date	Rev	File
EEM/TD/R Julio López Roldán				

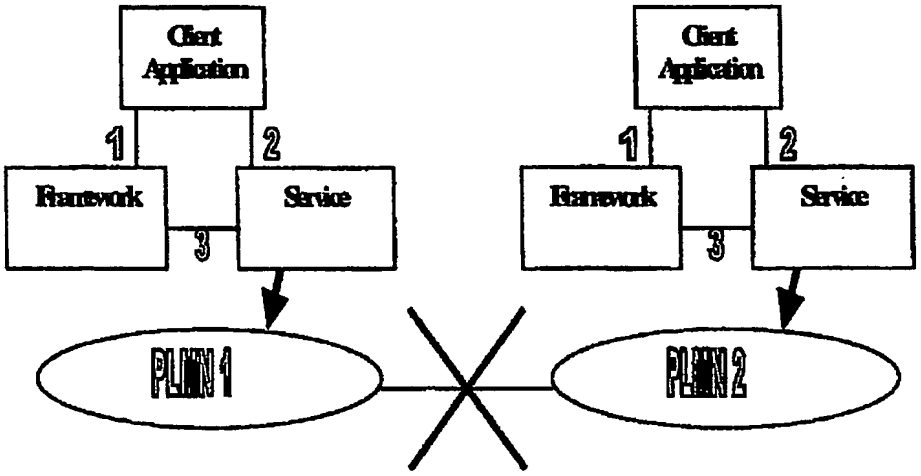
Interface classes between the Applications and the Framework, that provide applications with basic mechanisms (e.g. Authentication) that enable them to make use of the service capabilities in the network. Interface classes between Applications and Service Capability Features (SCFs), which are individual services that may be required by the client to enable the running of third party applications over the interface e.g. Messaging type service. Interface classes between the Framework and the Service Capability Features, which provide the mechanisms necessary for multi-vendorship.
These interfaces represent interfaces 1, 2 and 3 of the Figure below.



1.5 Problem

The problem that will be solved in this invention is related to the **execution of applications in the Home Network that uses network services from an heterogeneous visited network through the OSA/PARLAY interface.** The application will be isolated from the negotiation between the home network and the visited one, that negotiation will be carried out by the Frameworks.

Uppgjord (även fakt.ansvarig om annan) - Prepared (also subject responsible if other)		Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062		
Dokansv/Godk - Doc respons/Approved	Kontr - Checked	Datum - Date	Rev	File
EEM/TD/R Julio López Roldán				



In the figure it is shown how the access to remote services should be not done by the core networks because of the great diversity of access methods to the features. The access to the remote services must be done through the SCSs of the other network because that SCS knows how to manage its services and the open interface is common independently of the core network.

As an example of concrete problems we can expose two related with positioning issues.

1. - An international parcel company wants to track their trucks not only in its country but also in other countries. The client application has no knowledge about the network where the mobile terminal is but this functionality is key for this company as an international parcel company.

2. - An international healthcare company X that wants to track their heart patients not only through the wide area PLMN networks but also within indoor spaces i.e. within hugh airports using Bluetooth positioning technology or within underground facilities without a PLMN network but with WLAN coverage. The WLAN can be located in the same or different country, and the HPLMN and the WLAN operator must have an agreement. The healthcare client application has no knowledge about the network where the patient's mobile terminal is when it ask for a customer localisation, but this functionality is key for this company just to follow up their customers or to receive his hearth device alarms.

Today these two problems have not possible solution for all the networks because, even though the network has an OSA/Parlay interface this interface only works on top of the local core network. This invention wants to solve this

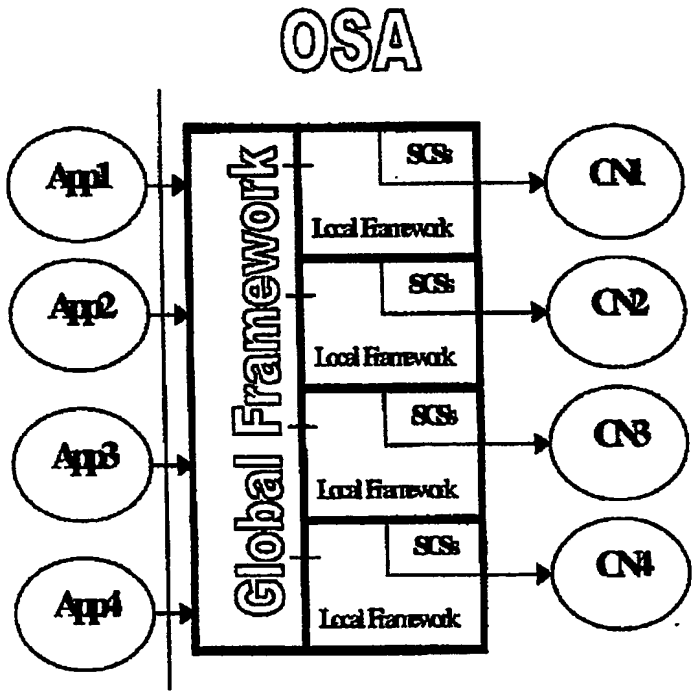
Uppgjord (även fakt.ansvarig om annan) - Prepared (also subject responsible if other)	Nr - No.	
EEM/TD/R Alejandro Bascuñana Muñoz	EEM/TD/R-02:062	
Dokansv/Godk - Doc respons/Approved / Kontr - Checked	Datum - Date / Rev	File
EEM/TD/R Julio López Roldán		

problem in the OSA/Parlay environment by allowing the communication among several OSA/Parlay frameworks.

Solution

The key contribution will be related to the extension of the OSA/Parlay framework signalling system to work in a multi-OSA environment. We will define new Interface classes between the Frameworks in order to manage the global roaming. It can be summarised the main goal of our invention in the following sentence: **adding a new framework-to-framework interface in order to have access to the service capability servers of other networks through OSA/PARLAY environments.**

In the following figure it can be seen how several applications need to access to services distributed along several core networks, and we introduce a "Virtual" Global Framework (VGF) that will manage the access of those applications to the services in other networks.

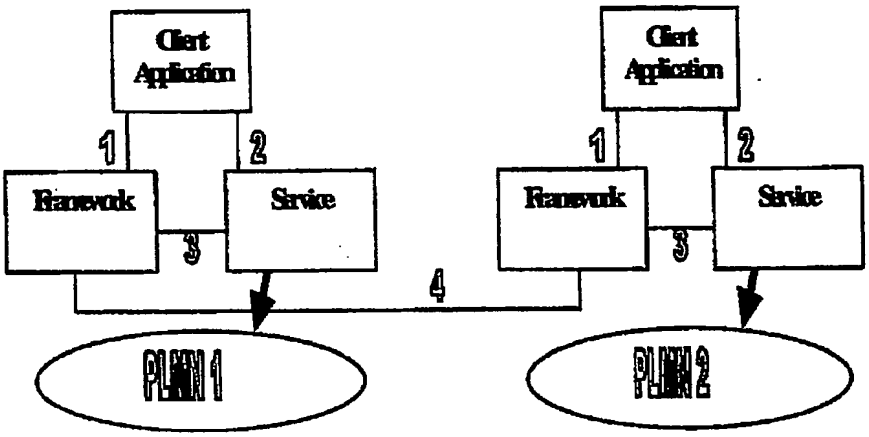


One "virtual" global framework.

Read and Understood by: ..... Date: .....

Read and Understood by: ..... Date: ..... Template invdisclsdot version 1 (1999-12-01)

Upprätt (även fakta ansvarig om annan) • Prepared (also subject responsible if other)	Nr - No.	
EEM/TD/R Alejandro Bascuñana Muñoz	EEM/TD/R-02:062	
Dokansv/Godk - Doc respons/Approved / Kontr - Checked	Datum - Date / Rev	File
EEM/TD/R Julio López Roldán		



The definition of a framework-to-framework interface,as can be seen in the picture, will allow remote service execution and service network roaming. To solve the problem addressed in the last section the following steps will be done:

1. Application will ask for a service to its local framework
2. If the mobile terminal is not located within its home network, application will ask to the local framework how to use the service in the visited network.
3. The local framework will contact to the visited one in order to allow the use of the remote service by the local application, all the negotiation will be performed by the home and remote frameworks.
4. The visited Frameworks have to communicate to the local framework the instance ID of the service.
5. The application will ask to the remote SCF about the service.

The "Virtual" Global Framework can be implemented following several ways in the registration phase among the frameworks:

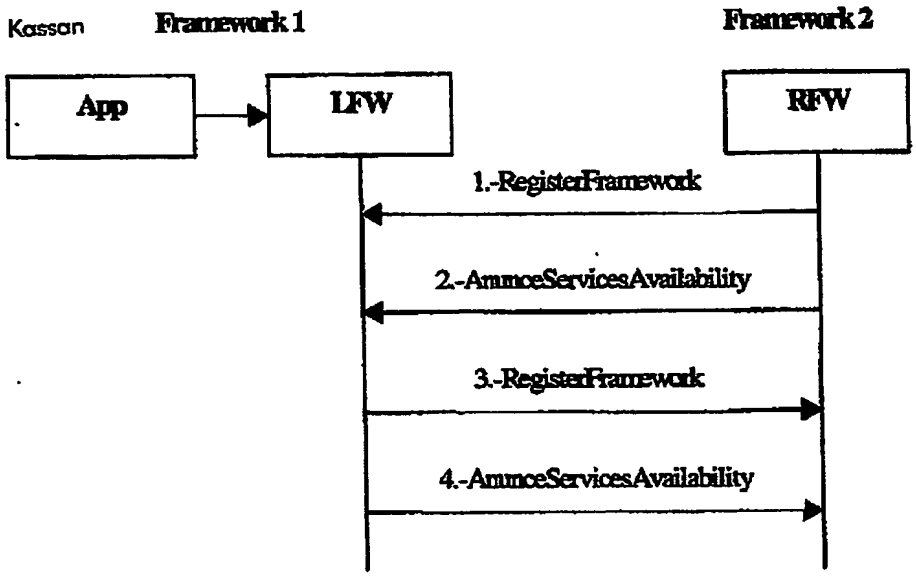
1. - Frameworks interchange and refresh information about their services and interfaces in an off-line mode.
2. - Home Network Framework asks, in an on-line mode, to the visited Framework about services and interfaces before access to the services in the visited network.

Read and Understood by: ..... Date:.....

Read and Understood by: ..... Date:.....

Uppgjord (även ladsansvarig om annan) - Prepared (also subject responsible if other)		Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062		
Dokansv/Godk - Doc respons/Approved	Kontr - Checked	Datum - Date	Rev	File
EEM/TD/R Julio López Roldán				

In this invention disclosure we will study in depth the first case.
First of all it will be explained the register phase among the Frameworks:



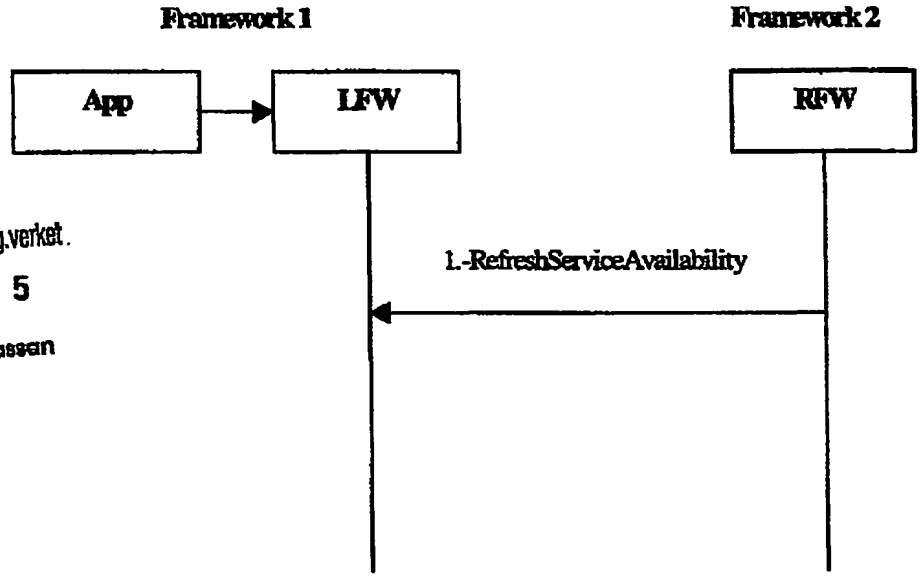
Register new associate framework

As can be seen in the figure the register process between frameworks can be summarised into 2 basic steps.
The first one advertises the existence of a new framework (Remote) that can be accessed by the framework of the operator that has the application (Local).
The second step publish the interfaces that will allow to the Local Framework the access to the services in the Remote Framework
The new Framework references and the available services will be stored in the framework. When the framework adds or changes services the framework will send an update of the service to associate frameworks.

Read and Understood by: ..... Date:.....

Read and Understood by: ..... Date:.....

Uppgjord (även fakaansvarig om annan) - *Prepared (also subject responsible if other)*		Nr - *No.*		
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062		
Dokansv/Godk - *Doc respons/Approved*	Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán				

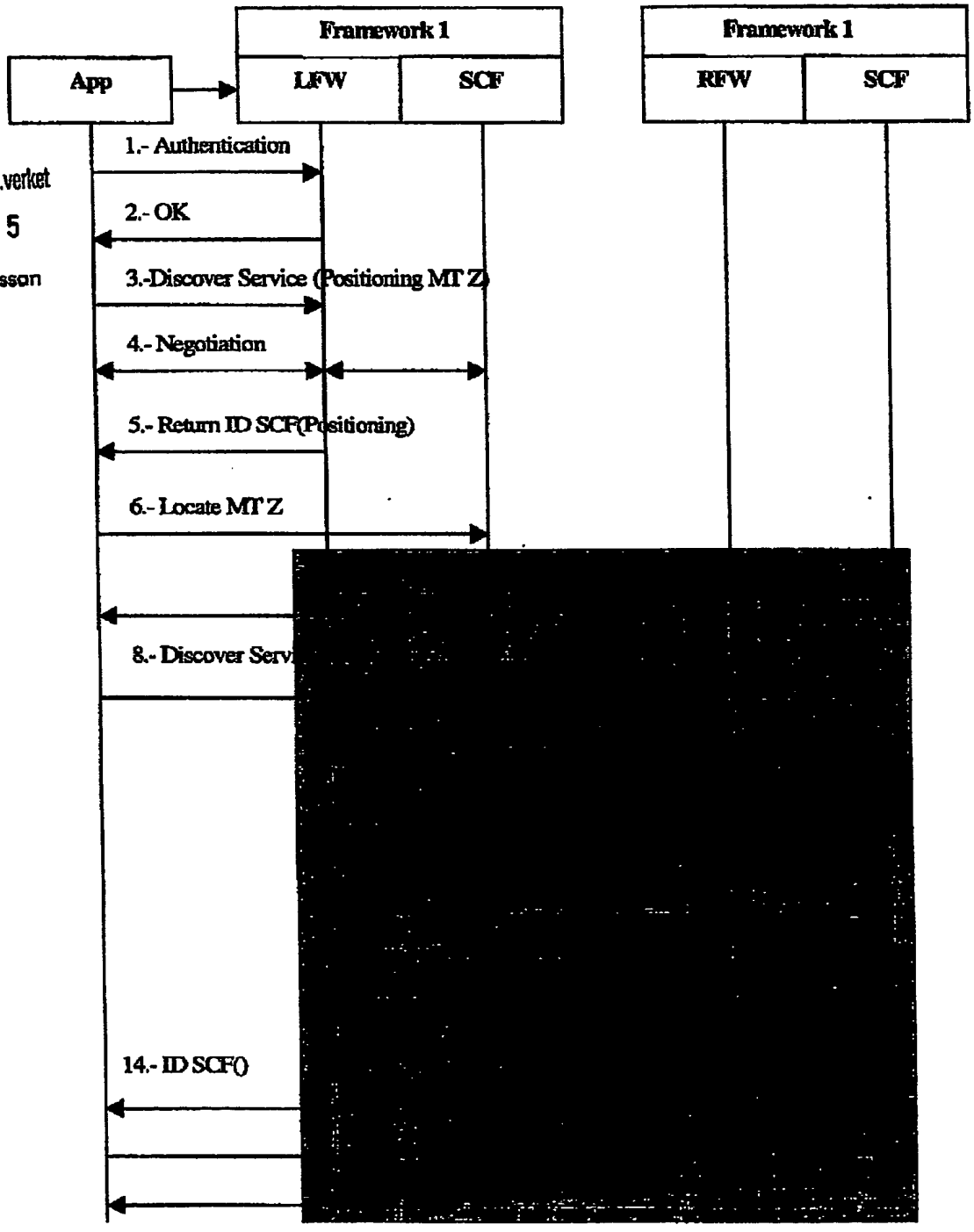


The following sequence diagram shows the steps in the case of the use of a localisation service in a visited network:

Read and Understood by: ..... Date: .....

Read and Understood by: ..... Date: .....

Uppgjord (även fakt.ansvarig om annan) - *Prepared (also subject responsible if other)*		Nr - *No.*		
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062		
Dokansv/Godk - *Doc respons/Approved*	Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán				



Read and Understood by: ..... Date: .....

Read and Understood by: ..... Date: ..... Template invdisc1.dot version 1 (1999-12-01G)

Uppgjord (även fakta ansvarig om annan) - *Prepared (also subject responsible if other)*		Nr - *No.*	
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062	
Dokansv/Godk - *Doc respons/Approved*	Kontr - *Checked*	Datum - *Date*	Rev	File
EEM/TD/R Julio López Roldán				

It can be seen the OSA application in blue. The applications have to access to a service, and don't know in which network the MT is. In the sequence diagram the service accessed is a localisation service.
In green can be seen the frameworks and the associate SCFs.
In orange are remarked the features that must be changed in the OSA/PARLAY model just to provide the new roaming functionality.

First of all the application contacts the framework, gets authenticated (1,2) and request for the discovery interface (..). The framework returns a reference to the Discovery interface after which the application uses this interface to request for the positioning SCF and the special capabilities it needs (3). At this moment the framework checks whether the application is allowed to use the SCF and under which conditions. This is captured in the so-called Service Level Agreement (SLA) between the network operator and Service Provider. In case the application is allowed to use the SCF the framework returns all IDs of SCFs that could fulfill the needs of the application. Next the application selects one of these SCFs and the SCS then creates and SCF instance that is to be used by this application and also is able to check the conditions. The reference of this SCF instance is returned to the framework (4) and the framework returns the reference to the application (5). From this moment on the application is able to use the SCF.

The application ask for localisation the MT Z (6) and the SCF detects that the MT Z is localised at network R. This response is sent back to the application (7). The application then asks to the framework about the possible access to the remote SCFs (8). The process continues as follows: The Home Framework request for authentication (9,10) to the remote framework, and the Home Framework ask for the localisation service (11), the Home Framework selects one of these VSCFs requested by the application and negotiate capabilities (Home framework knows about application needs) (12) and the VSCS then creates a SCF instance in the visited framework that is going to be used by the application. The reference of this VSCF instance is returned to the Visited framework, the visited framework returns the reference to the home framework (13) and the home framework to the application (14). From this moment on the application is able to use the remote SCF, and the process has been managed by the frameworks.

The main advantage of this procedure is that the application only contact with its local framework each time it wants to access to a service and the framework manages the following process and the relationship with other federated OSA/PARALAY environments. The application only is registered in one framework and does not need to be registered in all the federated domains.

Read and Understood by: ..... Date:.....

Read and Understood by: ..... Date:.....

Uppgjord (även fakturansvarig om annan) - Prepared (also subject responsible if other)		Nr - No.		
EEM/TD/R Alejandro Bascuñana Muñoz		EEM/TD/R-02:062		
Dokansv/Godk - Doc respons/Approved	Kontr - Checked	Datum - Date	Rev	File
EEM/TD/R Julio López Roldán				

1.7 Merits of the invention

The invention provides a method that allows a flexible and modular way of communication among heterogeneous networks and a way to add new functionality to the networks.

Other relevant documents

1.- .OSA/Parlay Specifications ETSI ES 201 915-1 v1.1.1(2001-12) Open Service Access; Application Programming Interface; Part 1: Overview

2.- OSA/Parlay Specifications ETSI ES 201 915-2 v1.1.1(2001-12) Open Service Access; Application Programming Interface; Part 2: Common Data Definitions

3.- OSA/Parlay Specifications ETSI ES 201 915-3 v1.1.1(2001-12). Open Service Access; Application Programming Interface; Part 3: Framework

4.- OSA/Parlay Specifications ETSI ES 201 915-6 v1.1.1(2001-12). Open Service Access; Application Programming Interface; Part 3: Mobility SCF

5.- IEEE Communications Magazine. January 2000. JAIN: A New Approach to Services in Communication Networks.

6.-Ericsson White Paper. Opening the Networks with Parlay/OSA APIs: Standards and Aspects Behind The APIS. Ard-Jan Moerdijk and Lucas Klostermann

— END OF APPLICATION —

2002-11-05

Read and Understood by: ..... Date: .....

Read and Understood by: ..... Date: .....

FEDERATION IN OPEN SERVICE ARCHITECTURE AND OPEN MOBILE ARCHITECTURE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The field of the invention is within, but not limited to the area Service Network, Parlay / OSA. OSA is the abbreviation of Open Service Access which represents the concept of having standardized interfaces towards services and is practiced by Parlay (www.parlay.org) , 3GPP (www.3gpp.org) and ETSI (www.etsi.org)). Another area where the invention could be useful is OMA. OMA is the abbreviation of Open Mobile Alliance, which is a telecom and IT industry Standardization initiative to enable services to mobile end-users.

2. Related Art

3GPP "Open Service Access", Application Programming Interface, Part 3: Framework, 3G TS 29.198-3 v5.0.0, SAML (Security Assertion Markup Language) describes several types of Assertions and a protocol for handing out Assertions.

Certain operators of telecommunication networks are organised in such a way that there is an organisation / department that is responsible for the core network and related in house developed end-user services / applications and one or more other, separate, organisations that are responsible for providing end-user services through partners and offering capabilities (functions that an operator domain can offer to other domains) to these partners (see Figure 1). Usually, both domains or organisations need to be able to enforce their own policies and gather information/statistics independently. Also both domains want to be able to offer the Capabilities within their domain and the Capabilities within the other domain. (This is called Federation).

What is needed is a flexible solution where one domain (Donor Domain) offers Capabilities towards another domain (Receiver Domain) that in turn can offer these Capabilities to it's own partners or providers. The solution should also allow capturing of agreements between the different domains and having these Agreements enforced. Solutions like Parlay/OSA allow an operator to offer Capabilities to application providers in a secure, controlled manner: the operator can define so-called Service Level Agreements or policies that can be enforced during run-time.

However, in the original outset, Parlay/OSA (Open Service Access) has not focussed on an architecture where one domain offers it's Capabilities to another domain and vice versa and where both domains have their own partners that provide the applications where both domains need to be able to install Service Agreements and have these enforced.

Within state-of-the art Parlay/OSA there exists the concept of enterprise operator, a role that is allowed to define in the operator domain, Service Agreements between the enterprise operator and application providers. The enterprise operator is bounded by a Service Agreement between the operator and the enterprise operator this is called a Service Contract. However there is no support for the case where one domain wants to offer Service Enablers of another domain to it's application providers through its own Framework under the conditions of the Service Agreement between the two domains (shown in Figure 2).

SUMMARY OF THE INVENTION

The present invention outlines the different possibilities to overcome the limitations and allow every domain to install and enforce its policies.

Three main embodiments will solve the mentioned problem.

The first one is to extend the existing Service Agreement model and allow a Receiver Domain to 'partition' the Service Agreement between the donor and receiver. The partitions make up the Service Agreements between the receiver and it's application providers. The second one is to have a model where the Receiver Domain has a so-

called Proxy Enabler for each enabler of the Donor Domain. The third embodiment presents a more flexible solution based on Assertions in stead of the current Service Agreement model.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the situation where operators are organised in such a way that there is an organisation / department that is responsible for the core network and related in house developed end-user services / applications and another, separate, organisation that is responsible for providing end-user services through partners and offering Capabilities to these partners.
FIG. 2 shows a situation according to the current art showing that it is impossible where one domain wants to offer Service Enablers of another domain to its application providers through its own Framework under the conditions of the Service Agreement between the two domains.
FIG. 3 shows an embodiment using state-of-the-art. Here, the operator domain 1 takes on the role of Enterprise operator to the Operator 2 domain in order to setup and define Service Agreements for the application providers within the domain of Operator 1. Service access is obtained through the Framework of Operator 2 i.e. the same domain as the domain that offers the Services.
FIG. 4 shows the present invention. Here, Operator 1 can be the IT department that has contracts with the application providers and Operator 2 can be the core network department.
FIG. 5a to 5f show the method within a Framework Federation – Service Agreement Partitioning.
FIG. 5a shows how Service Level Agreement are advertized to receiver Frameworks.
FIG. 5b shows how a Federation Service Profile is created.
FIG. 5c shows how a Federated SCF is installed in a Receiver Framework.
FIG. 5d shows how Federation Service Level Agreements are signed.
FIG. 5e shows how Apllication Service Level Agreements are signed.
FIG. 5f shows how Federation Service Level Agreements are terminated.
FIG. 6a to 6d show the method of providing Service Access in a Federation Context by means of a Proxy SCS.
FIG. 6a shows how a Proxy is installed.
FIG. 6b shows how an Application Service Level Agreement is signed and the Proxy SCS relays requests to the real SCS while enforcing the local policies of the receiver domain.
FIG. 6c shows how a Service level Agreement is terminated.
FIG. 6d shows how the SCS is registered as Proxy alternative.
FIG. 7a to 7f show the method of having an Exchange Service Access Assertion in a Federation Context.
FIG. 7a shows how Service Types are advertized to a receiver Framework.
FIG. 7b shows how an Assertion Profile and Assertions are created.
FIG. 7c shows how the Donor Framework hands out Assertions to a Receiver Framework.
FIG. 7d shows how the Receiver Framework hands over Assertions to the Application..
FIG. 7e shows how the Receiver Application practices an Assertion.

THE PREFERRED EMBODIMENTS

Service Agreement Partitioning

In this embodiment the OSA Framework in the Donor Domain (short Donor Framework) can advertise Service Enablers (SCS) to applications that subscribed for notifications thereof, using state-of-the-art. Such an application can be the OSA Framework in the Receiver Domain (short Receiver Framework).

When a Receiver Domain offers Service Enablers from a Donor Domain to the Receiver Domains partners, two domains are said to form a Federation. In Figure 4 these domains are of Operator 1 and Operator 2. When a Receiver Framework offers Service Enablers that are advertized by a Donor Framework, the two frameworks are working in a Federation setup.
In a Federation setup the Donor Framework has the following responsibilities to:
- advertise new registered Service Enablers to registered Receiver Frameworks;
- provide a mechanism whereby a Receiver Framework can sign a Federation Service Agreement (a Federation Service Agreement is a contract between the donor and the receiver on the terms under which the receiver and its partners can use a specific Service Enabler);

- provide a mechanism whereby a Receiver Framework can request a Receiver Application Service Agreement from the Donor Framework for one of the Receiver Framework partner's applications within the limits set by the Federation Service Agreement. The terms of the Receiver Application Service Agreement are constructed by the Receiver Framework, the Donor Framework ensures that the requested Receiver Application Service Agreement is within the limits set by the terms of the Federation Service Agreement. The Receiver Application Service Agreement can be seen as a part of the Federation Service Agreement given to a specific Application . When an Receiver Application Service Agreement is given out to the Receiver Framework a new service instance is created and a reference is given to the Receiver Framework .

In a Federation setup the Receiver Framework has the responsibility to register Service Enablers (Donor Service) advertised by a Donor Framework and make them available for own applications. To be able to do this the properties of the advertised Service Enabler are retrieved from the Donor Framework. Service Profiles can be made for the Donor Services as for any other service in the receiver's domain.
However when an application selects such a Donor Service and signs the Service Agreement with the Receiver Framework the Receiver Framework requests the Donor Framework for a Receiver Application Service Agreement. In the request the Receiver Framework provides the terms/restrictions that are defined in the Service Profile that is assigned to the Receiver Application and the Donor Framework will use this to construct a Receiver Application Service Agreement.

Proxy model

In this embodiment there is a so-called Proxy Service Enabler in the Receiver Domain for each Service Enabler in the Donor Domain. This means that within the Receiver Domain an actual Service Enabler is present that proxies requests from applications to the Service Enabler in the Donor Domain and likewise in the other direction from the Service Enabler to the applications. From the viewpoint of the Service Enabler in the Donor Domain the Proxy Service Enabler is similar to an application.

In the Proxy setup the Donor Framework has the responsibility to:
Advertise new registered services to registered Receiver Frameworks
Optionally provide the Proxy Enabler code to the Receiver Domain so that it can be tuned and instantiated in the latter domain.

In the Proxy setup the Receiver Framework has the responsibility to:
Register Proxy Service Enablers and make them available for own applications. There are a number of alternatives to create a Proxy Service Enabler. One alternative is that the Proxy is a downloadable component from the Donor Domain. A second alternative is that the Proxy Service Enabler is constructed based on the Service Type and the property values of the real Service Enabler in the Donor Domain. Information about the Service Type and the supported property values can be obtained from the state-of-the art Framework. A third alternative is to deliver along with the Service Enabler software that basically implements / stubs the API the enabler is supposed to implement and is able to request the Donor Framework creation of a Service manager on the Service Enabler. The Receiver Domain can in this case add the necessary software to enforce the local policies and compile it to the target environment.

In the Proxy setup the Proxy Service Enabler has the responsibility to:
Maintain communication between the Proxy and the real SCS, proxy all requests from the application and relay them to the real SCS in the Donor Domain.Furthermore, the Proxy Service Enabler is responsible to enforce the policies / Agreements between the application providers and the Receiver Domain.

A specific case is when the Service Enabler is registered to the Framework of the receiver Domain to fulfill the role of Proxy Service Enabler.

The Handover of a service assertion and the practicing of a service Assertion

In this embodiment the OSA Framework in the Donor Domain (short Donor Framework) can advertise services (Donor Services) to applications that subscribed for notifications thereof, using state-of-the-art. Such an application can be the OSA Framework in the Receiver Domain (short Receiver Framework). The Receiver Framework would then request the hand out of a service Assertion by the Donor Framework. An Assertion is an authorization and/or authentication statement. It can contain a number of attributes. The Donor Framework hands out the service Assertion ('statement') to the Receiver Framework (or any other requesting system/entity (e.g an

application). The service Assertion describes an Agreement between *an* (any) application and a specific service. The Assertion can be sent to the service (is 'practice') and then the service becomes available to the one who sends – or practices – the Assertion. When the Assertion is *issued* it is not known which application or system/entity is going to practice that Assertion.

The Receiver Framework can advertise its obtained Capabilities (represented by the Assertion) and hand over the Assertion to an application inside or outside of the Receiver Domain. This application can then either practice the Assertion or hand the Assertion over to another application. This way, Agreements accompanied with the authorization rights to use a service according to that Agreement can be exchanged in a very flexible manner.

Additionally the system/entity (e.g. application) that hands over the Assertion can add authentication, authorization or attribute data to the Assertion. This way, the application can 'customize' the Assertion. Each domain that hands over the Assertion can hand out additional data and 'connect' that to the Assertion. It could e.g. extend the stated Capabilities with own Capabilities or restrict the stated Capabilities. The result is a 'layered' Assertion.

In a Federation setup the Donor Framework has the following responsibilities:
Advertize new registered services to registered Receiver Frameworks.
Create service Assertions that represent the Agreement and right for Donor Service usage.
Provide a mechanism to handout a service Assertion to the Receiver Framework. The mechanism involves signing by both parties of a statement that the Assertion is exchanged so that non-repudiation can be proved if necessary. Additionally the Assertion may be encrypted.
Keep track of handed out Assertions.
Handle requests for checking the validity of a practised Assertion. The requests are sent by the Donor Service. The Donor Framework must check whether the Assertion has not been practised before. An Assertion can only be practised once. The Donor Framework indicates to the service whether the Assertion is still valid or not.

In a Federation setup the Receiver Framework has the responsibility to:
Request the handout of a service Assertion.
Obtain the service Assertion from the Donor Framework. The mechanism involves signing by both parties of a statement that the Assertion is exchanged so that non-repudiation can be proved if necessary. Additionally the Assertion may be encrypted.
Advertise newly obtained Capabilities to the application in the Receiving Domain (and possibly also outside of the Receiving Domain).
Add authentication, authorization or attribute data to the Assertion: create a 'layered' Assertion.
Practice the Assertion (= provide the Assertion to the Donor Service). This typically happens when the Receiver Framework acts as a representative for the Receiver Domain, when the Receiver Domain has the intention to act as an enabler or middle layer towards other (partner) domains and shield the Capabilities of the Donor Domain.
or
Hand-over the service Assertion to a Receiver Application upon request of the Receiver Application. The mechanism involves signing by both parties of a statement that the Assertion is exchanged so that non-repudiation can be proved if necessary. Additionally the Assertion may be encrypted. When the Receiver Framework has handed over the service Assertion it is no longer allowed to practice the Assertion itself. The Receiver Application can then practice the assertion.

The (Donor) Enabler/SCS has the responsibility to:
Register with the Donor Framework.
Validate whether the assertion has been signed by the Donor Framework and (optionally) whether the assertion was not modified, or query the Donor Framework upon reception of an Assertion (when it received that Assertion for the first time) to validate whether the Assertion had been handed out by the Donor Framework and is (still) valid. The Donor Framework then responds with an acceptation or with a denial. When the Assertion is accepted, the Donor enabler/SCS grants the practitioner access to its service according the Agreement properties described in the Assertion.

We claim as our invention:

1. A method of extending existing Service Level Agreements between Donor Domains and Receiver Domains in a telecommunication network with multiple domains, the method comprising the steps of:
   - creating and assigning a Federation Service Profile on a Donor Framework;

- signing a Federation Service Agreement on a Donor Framework;
- installing (registering) a Donor Service in a Receiver Framework;
- requesting a Receiver Application Service Agreement from a Donor Framework

2. A method according to claim 1 wherein a Receiver Application Service Agreement serves as a partition of a Federation Service Agreement

3. A method according to claim1 wherein each domain is operated by a different operator

4. A method of constructing an ad hoc Proxy based on the information when a Service Enabler registers to a Donor Framework, the method comprising:

- downloading a Proxy from a Donor Domain; and
- allowing an operator of a Donor Domain to register an SCS as Proxy to a Receiver Domain.

5. A method according to claim 4 wherein the information comprises service type and or supported property values

6. A method of handing out and or handing over an Assertion that gives a practitioner the right to use a certain service in a federated framework setup, the method comprising the steps of:

- handing out an Assertion by a Donor Framework to a Receiver Framework;
- handing over an Assertion by a Receiver Framework to any other entity;
- signing an Agreement about the hand-out and or hand-over of an Assertion;
- requesting an Assertion; and
- a Donor enabler /SCS checking the validity of a received Assertion with a Donor Framework.

7. A method of practitioning an Assertion according to claim 6.

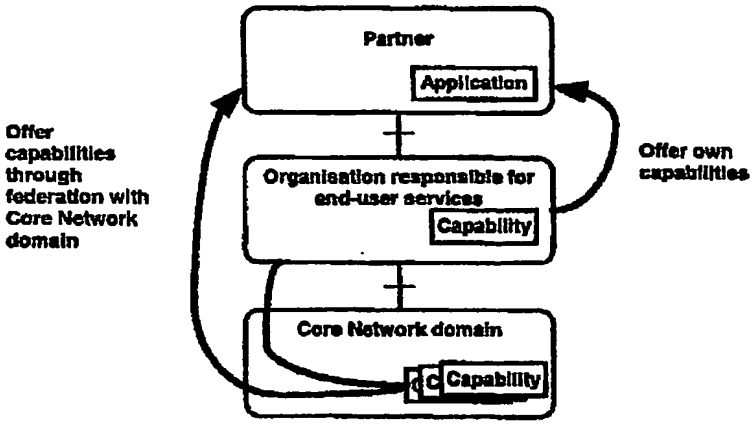


FIG. 1

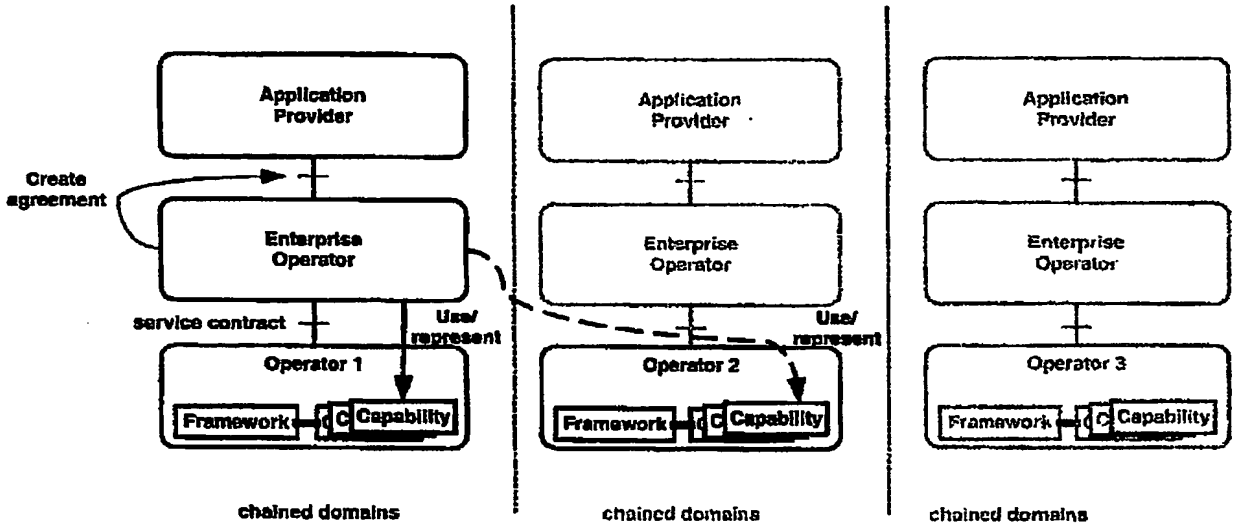


FIG. 2

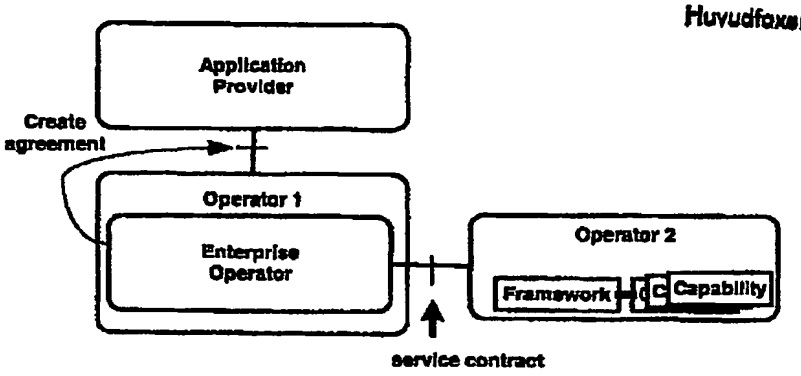


FIG. 3

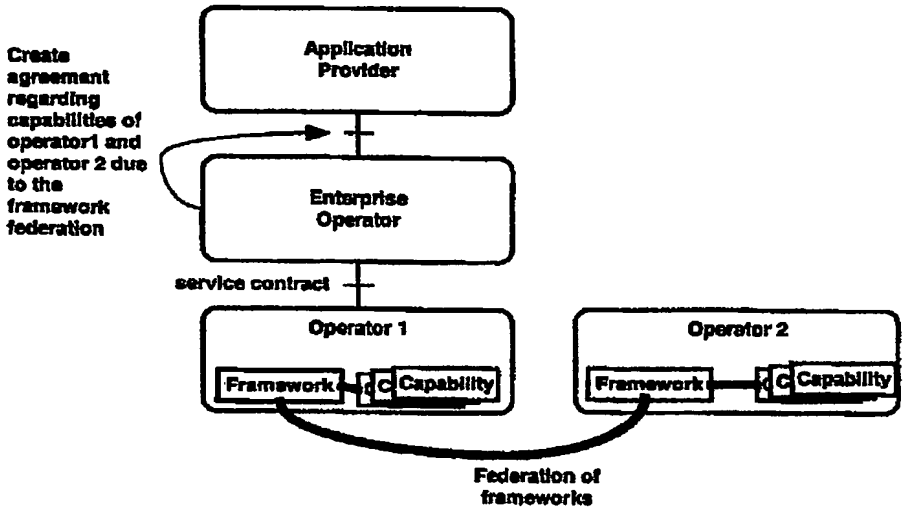


FIG. 4

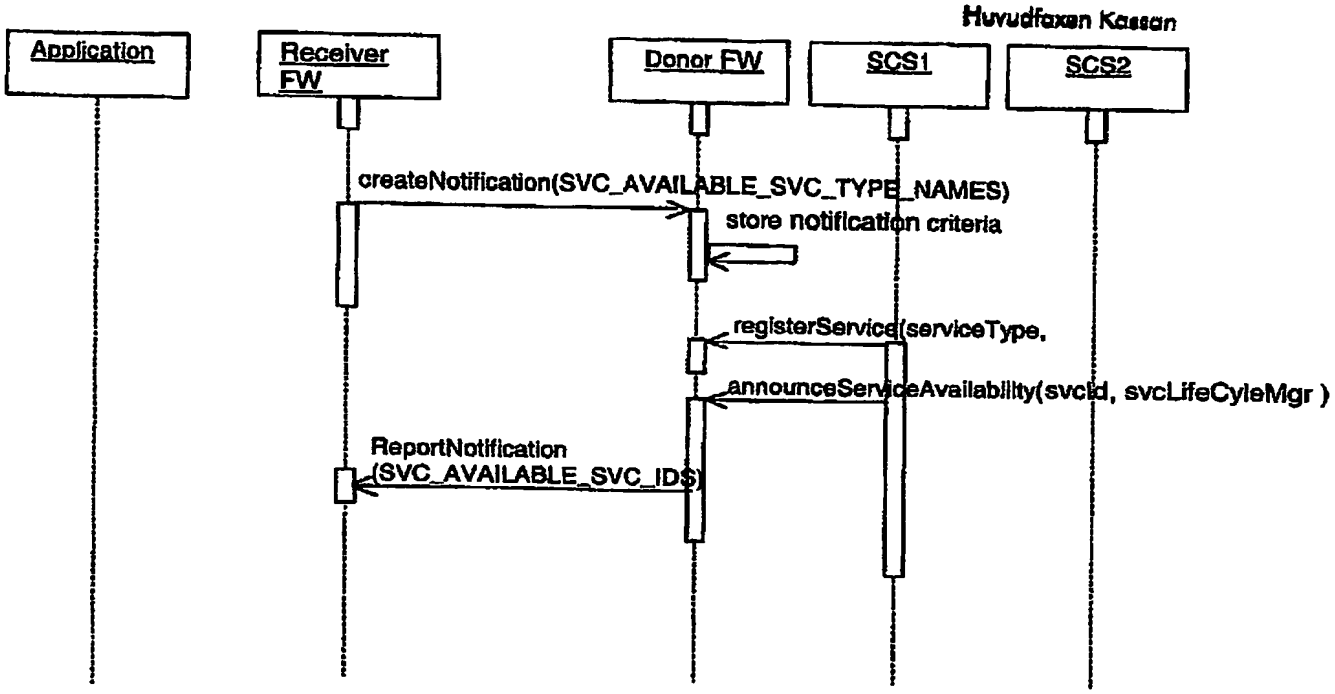


Fig. 5a

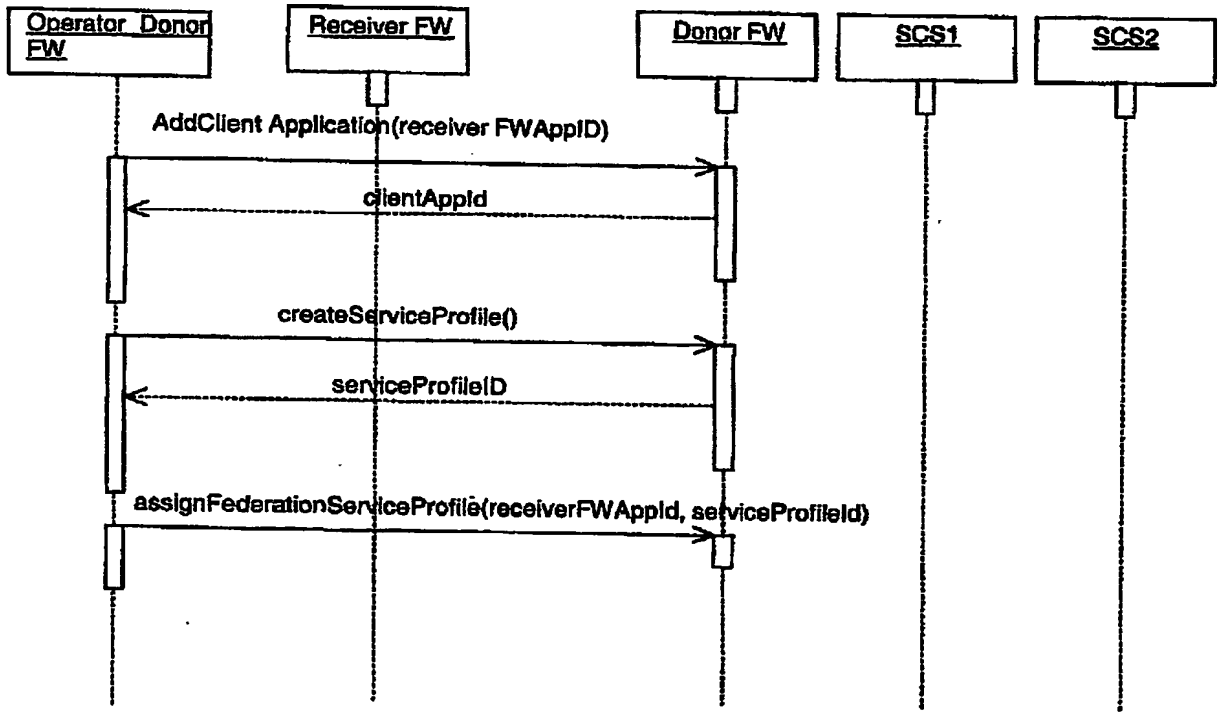


Fig. 5b

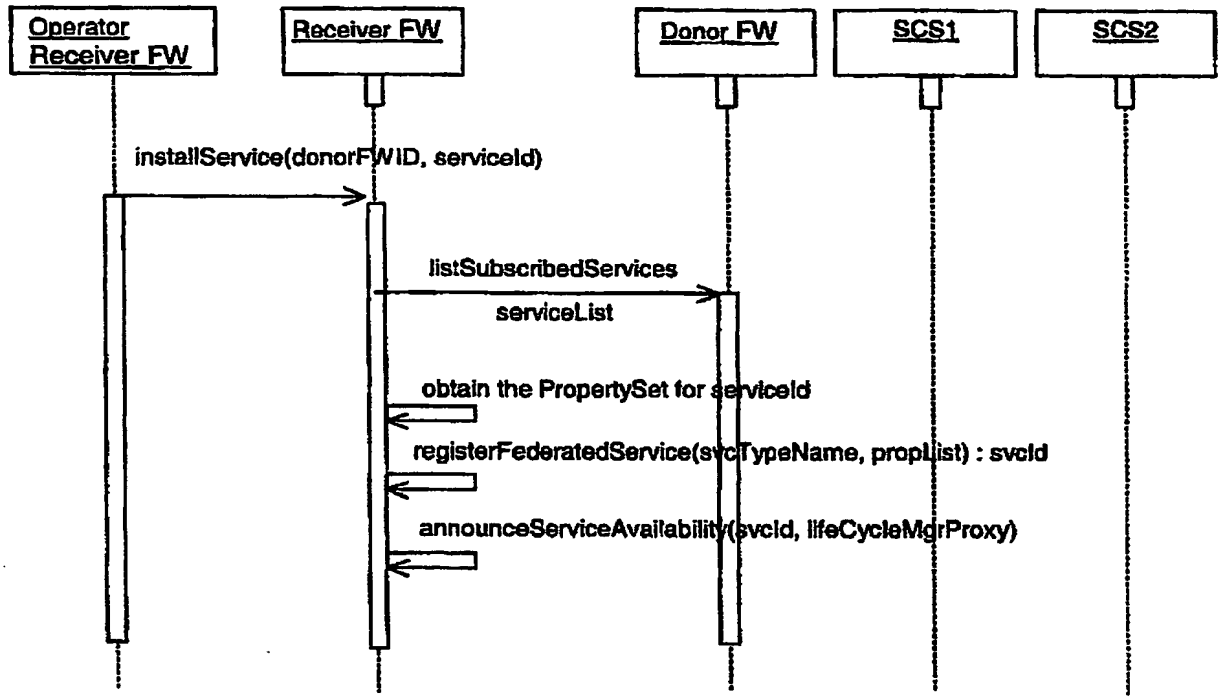

Operator Receiver FW
Receiver FW
Donor FW
SCS1
SCS2
installService(donorFWID, serviceId)
listSubscribedServices
serviceList
obtain the PropertySet for serviceId
registerFederatedService(svcTypeName, propList) : svcId
announceServiceAvailability(svcId, lifeCycleMgrProxy)

Fig. 5c

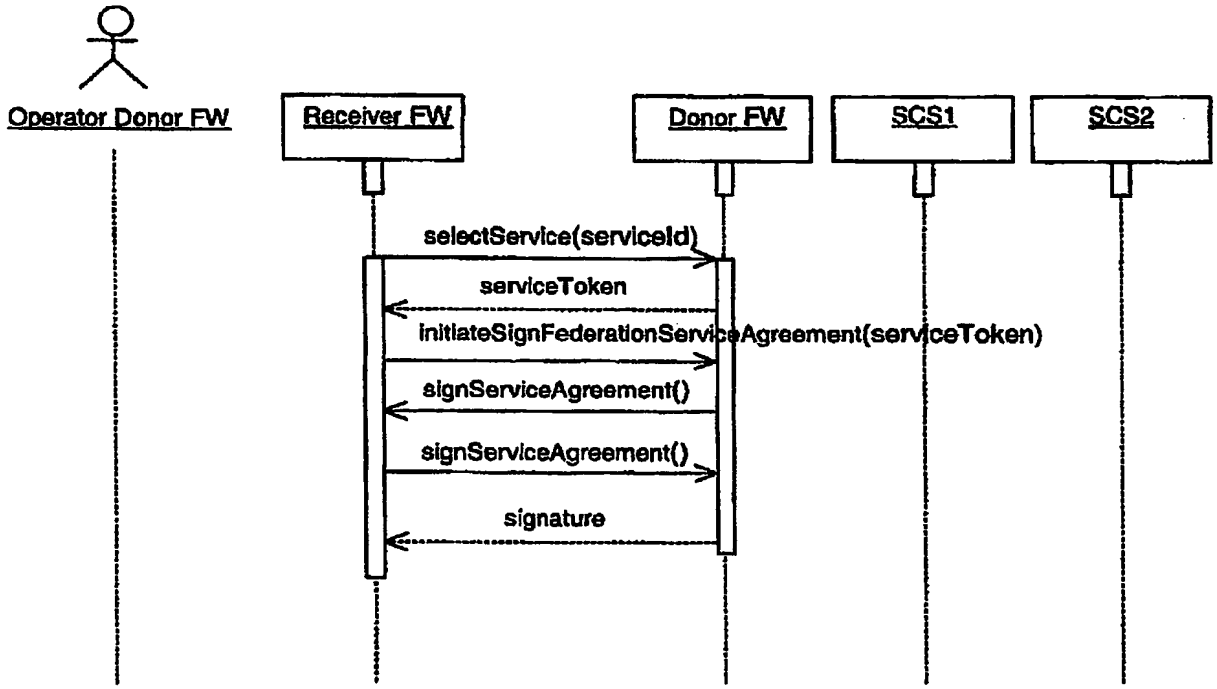

Operator Donor FW
Receiver FW
Donor FW
SCS1
SCS2
selectService(serviceId)
serviceToken
initiateSignFederationServiceAgreement(serviceToken)
signServiceAgreement()
signServiceAgreement()
signature

Fig. 5d

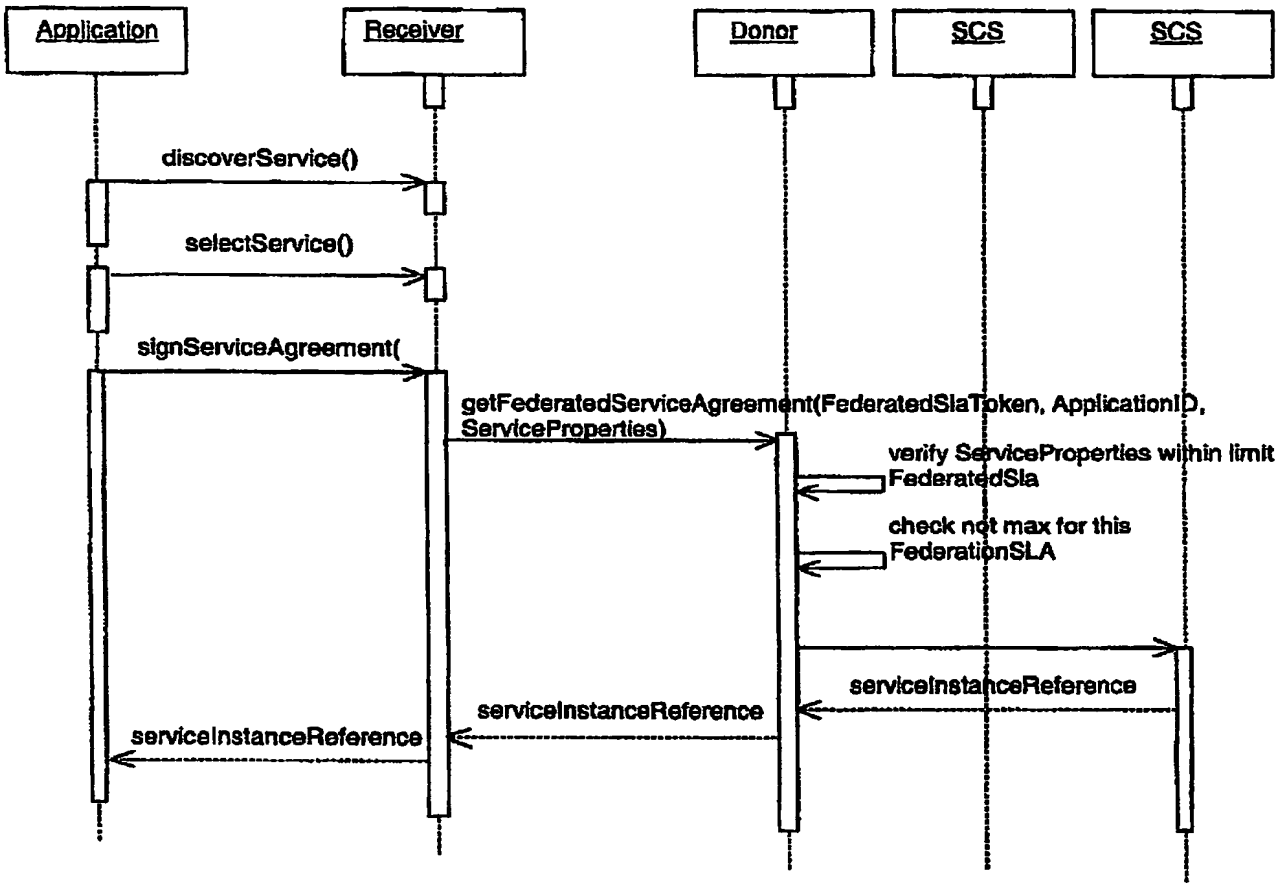


Fig. 5e

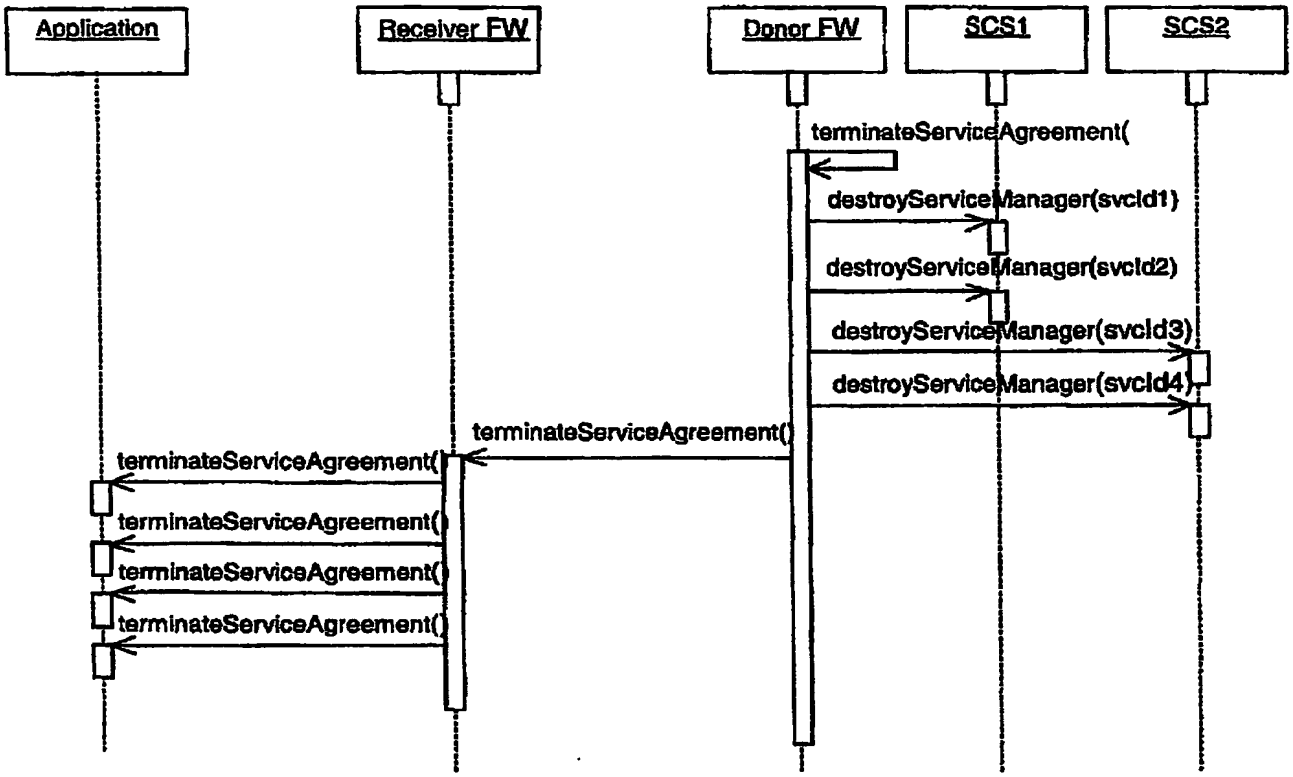

Application
Receiver FW
Donor FW
SCS1
SCS2
terminateServiceAgreement(
destroyServiceManager(svcId1)
destroyServiceManager(svcId2)
destroyServiceManager(svcId3)
destroyServiceManager(svcId4)
terminateServiceAgreement()
terminateServiceAgreement()
terminateServiceAgreement()
terminateServiceAgreement()
terminateServiceAgreement()

Fig. 5f

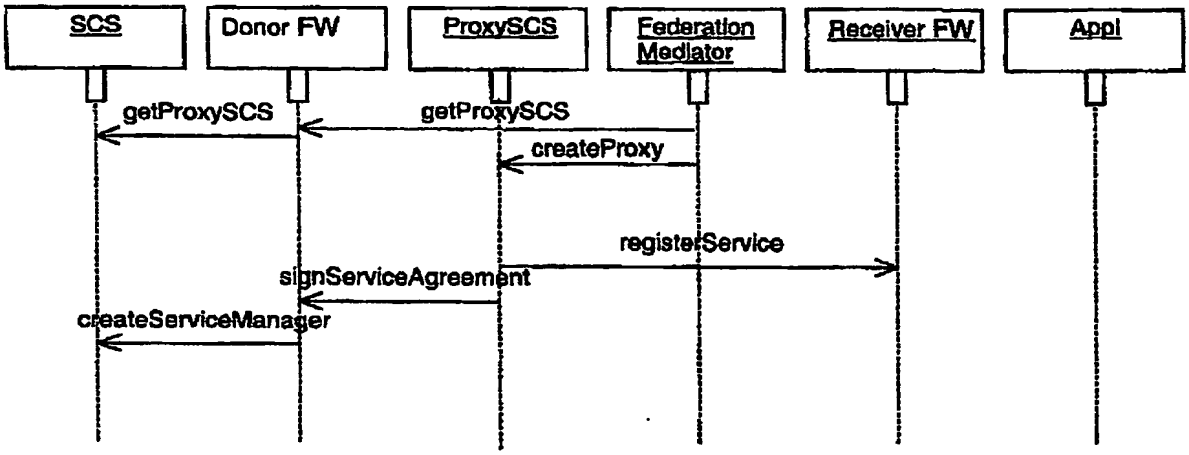

SCS
Donor FW
ProxySCS
Federation Mediator
Receiver FW
Appl
getProxySCS
getProxySCS
createProxy
registerService
signServiceAgreement
createServiceManager

Fig. 6a

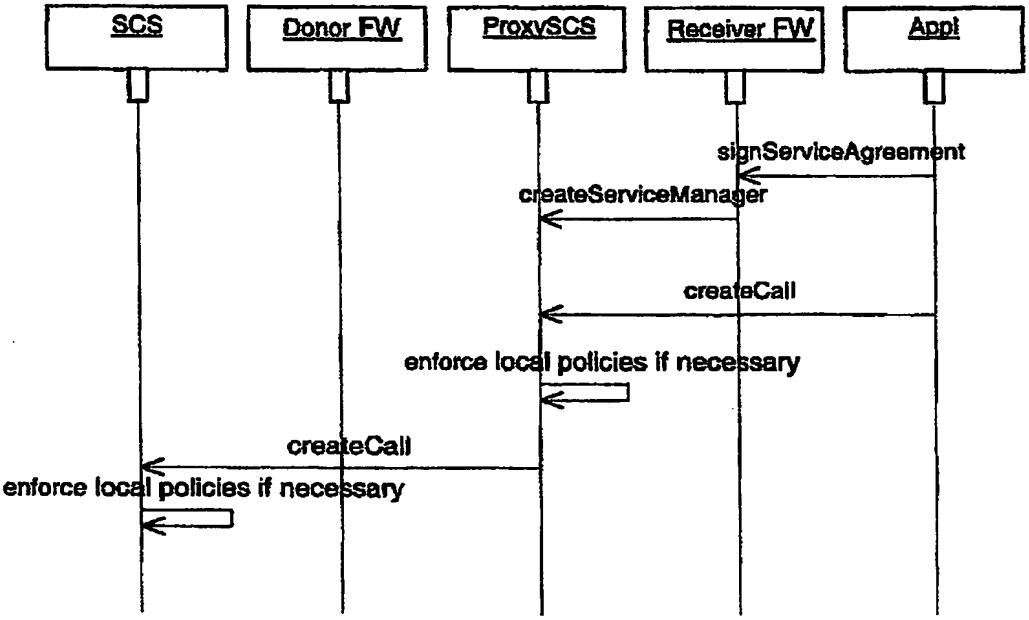

SCS
Donor FW
ProxySCS
Receiver FW
Appl
signServiceAgreement
createServiceManager
createCall
enforce local policies if necessary
createCall
enforce local policies if necessary

Fig. 6b

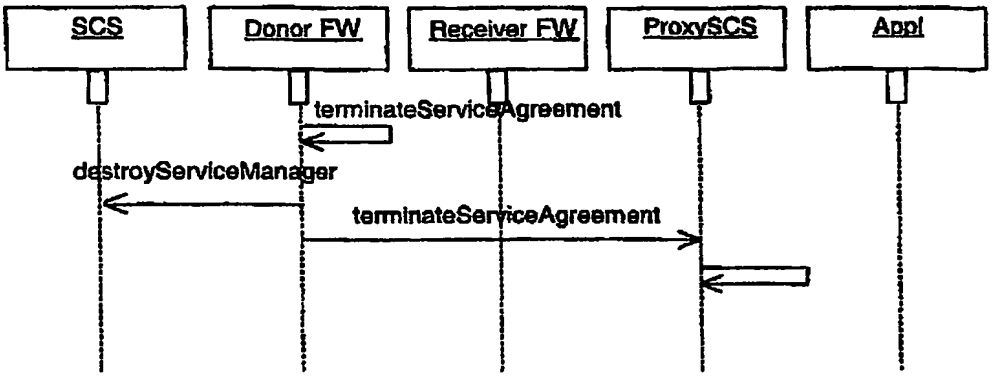

SCS
Donor FW
Receiver FW
ProxySCS
Appl
terminateServiceAgreement
destroyServiceManager
terminateServiceAgreement

Fig. 6c

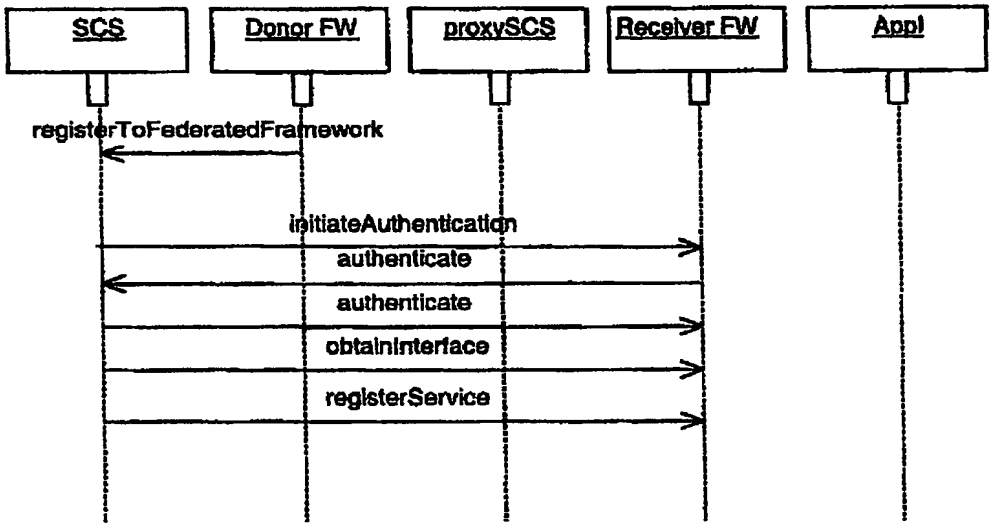

SCS
Donor FW
proxySCS
Receiver FW
Appl
registerToFederatedFramework
initiateAuthentication
authenticate
authenticate
obtainInterface
registerService

Fig. 6d

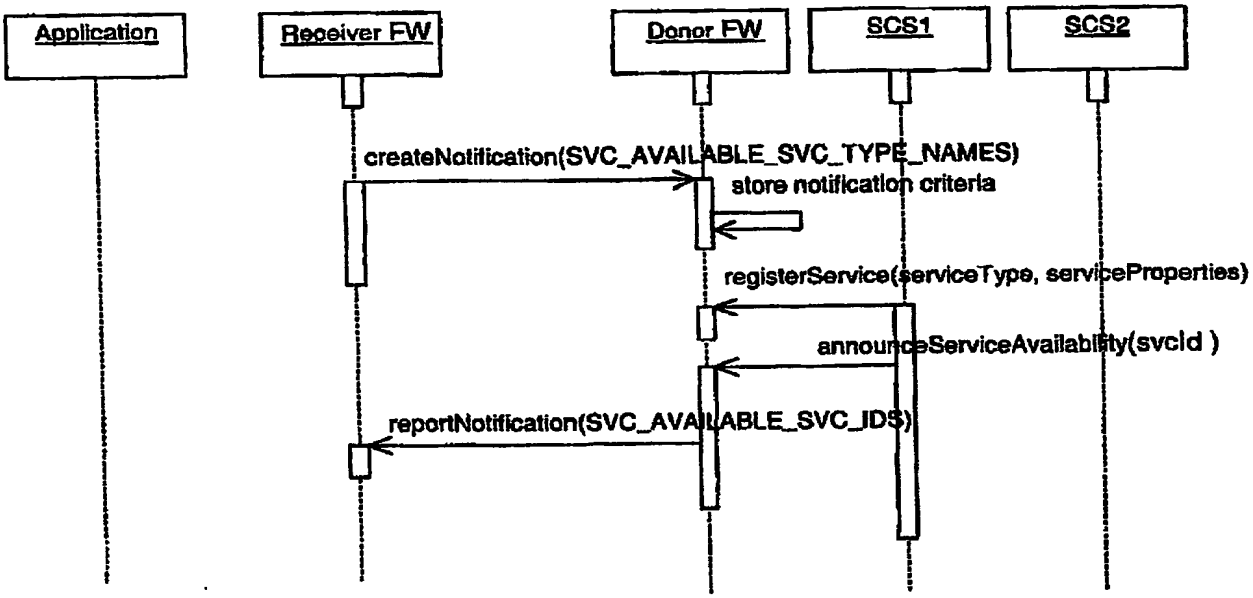

Application
Receiver FW
Donor FW
SCS1
SCS2
createNotification(SVC_AVAILABLE_SVC_TYPE_NAMES)
store notification criteria
registerService(serviceType, serviceProperties)
announceServiceAvailability(svcId)
reportNotification(SVC_AVAILABLE_SVC_IDS)

Fig. 7a

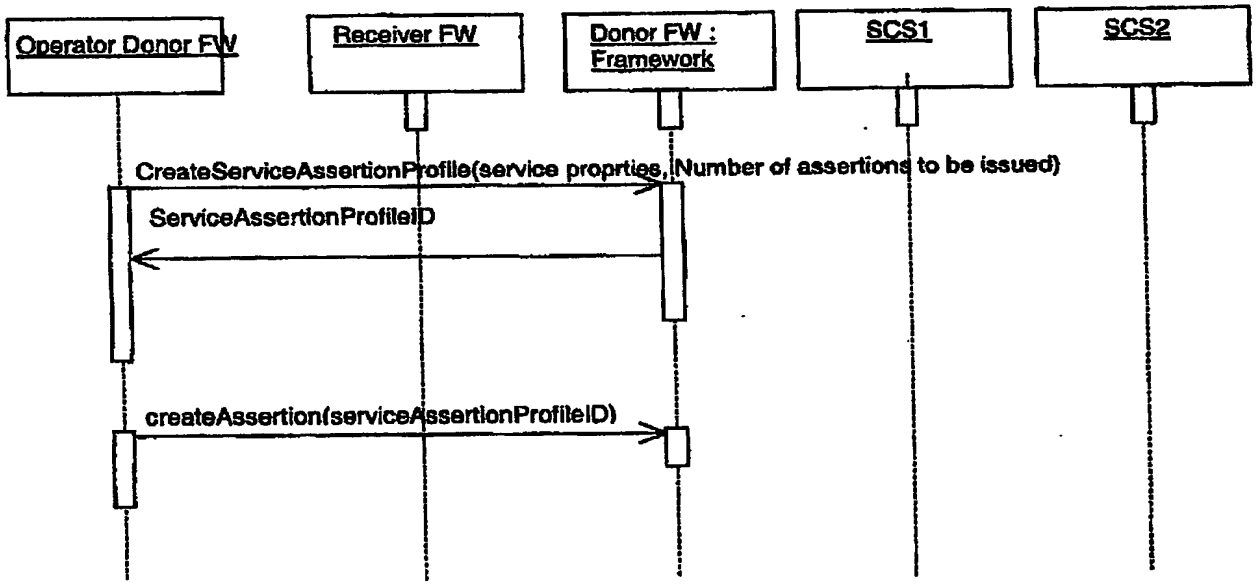

Operator Donor FW
Receiver FW
Donor FW : Framework
SCS1
SCS2
CreateServiceAssertionProfile(service proprties, Number of assertions to be issued)
ServiceAssertionProfileID
createAssertion(serviceAssertionProfileID)

Fig. 7b

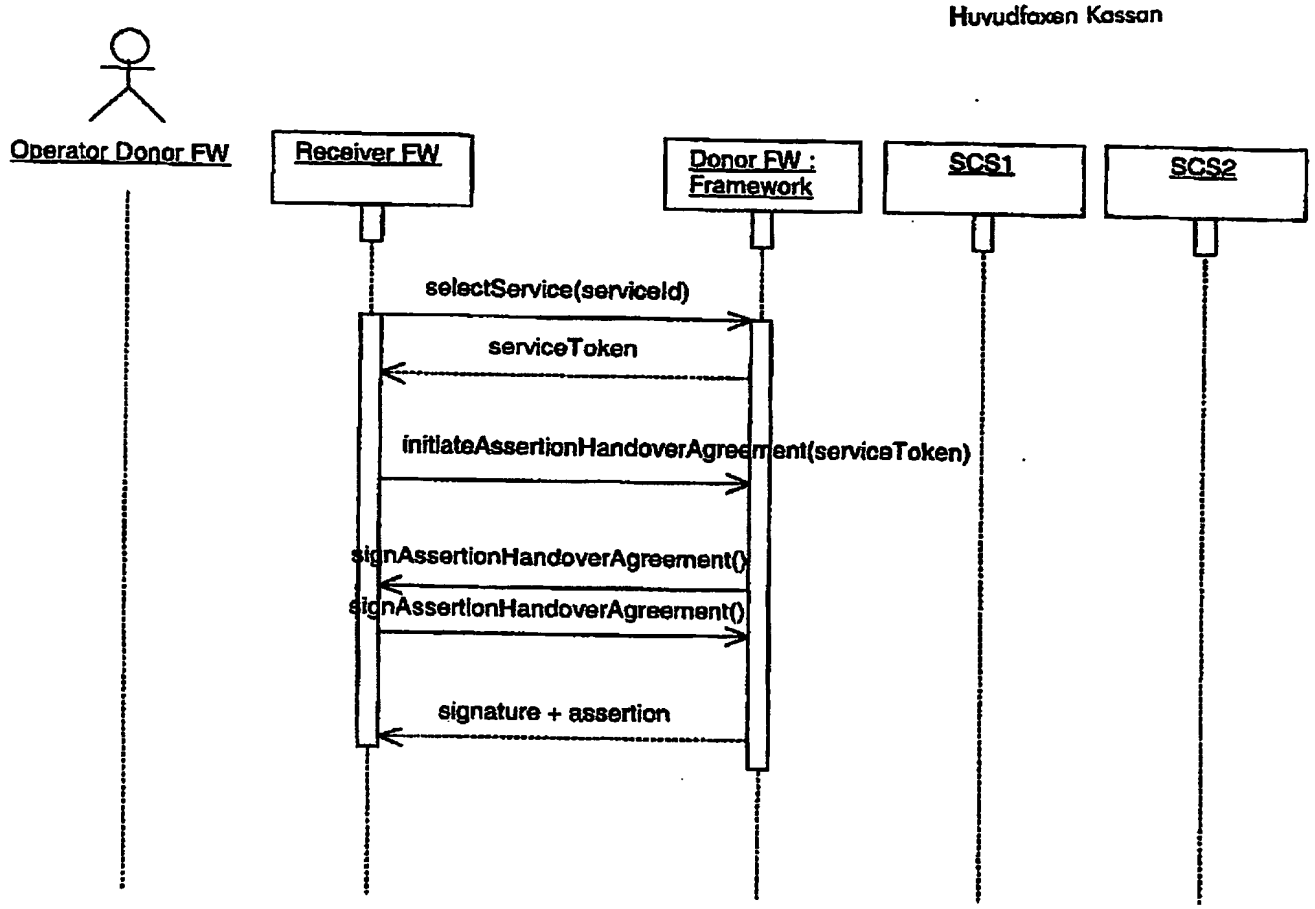

Operator Donor FW
Receiver FW
Donor FW : Framework
SCS1
SCS2
selectService(serviceId)
serviceToken
initiateAssertionHandoverAgreement(serviceToken)
signAssertionHandoverAgreement()
signAssertionHandoverAgreement()
signature + assertion

Fig. 7c .

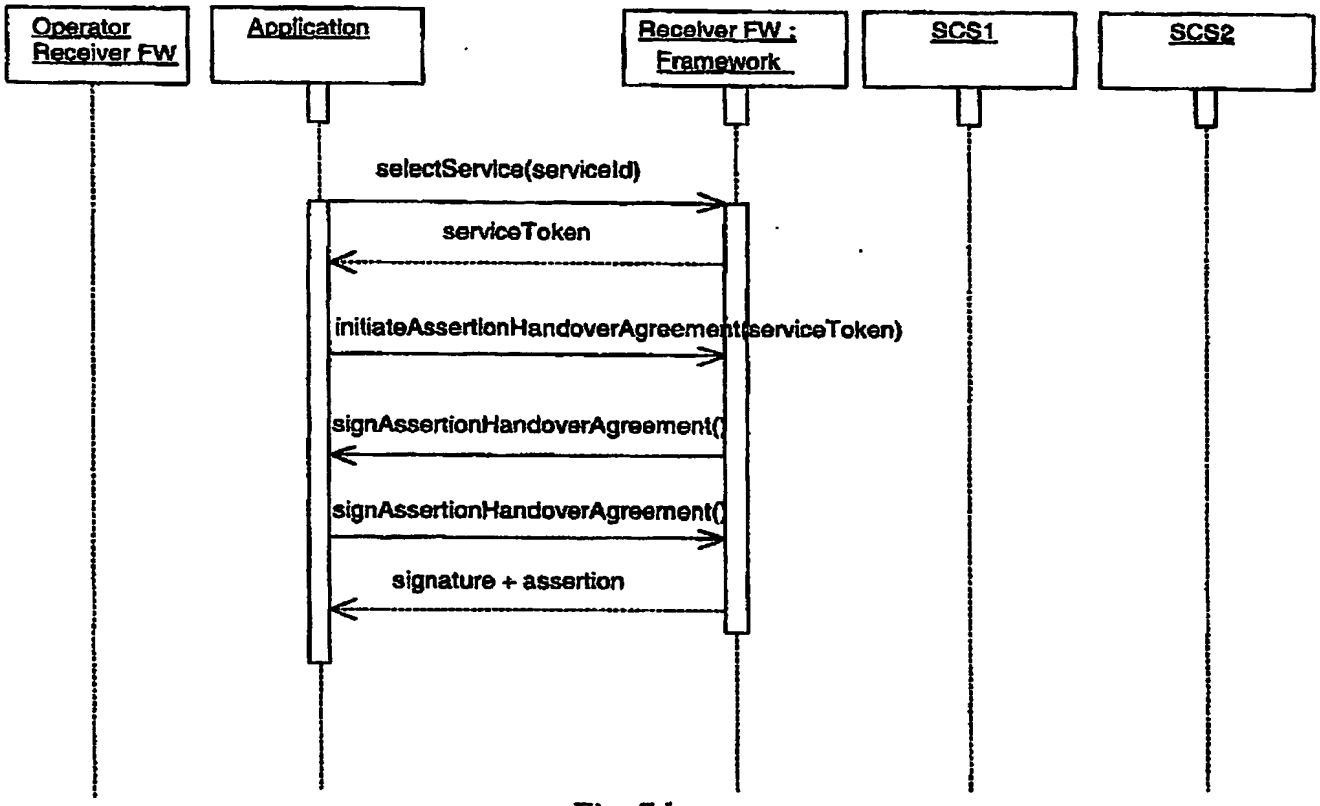

Operator Receiver FW
Application
Receiver FW : Framework
SCS1
SCS2
selectService(serviceId)
serviceToken
initiateAssertionHandoverAgreement(serviceToken)
signAssertionHandoverAgreement()
signAssertionHandoverAgreement()
signature + assertion

Fig. 7d

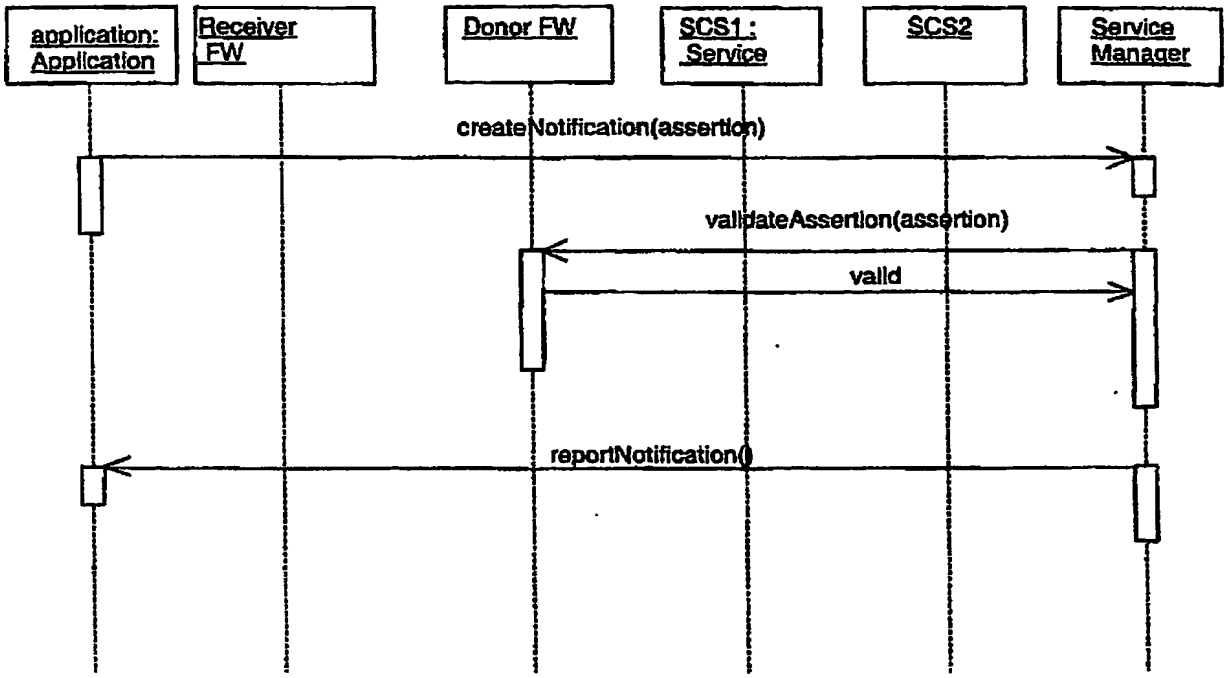

application: Application
Receiver FW
Donor FW
SCS1 : Service
SCS2
Service Manager
createNotification(assertion)
validateAssertion(assertion)
valid
reportNotification()

Fig. 7e

TERMINOLOGY & ABBREVIATIONS

Federation	A bond of domains based on Agreements to offer each other's services.
Donor Domain	A domain that provides (a) Service Enabler(s).
Receiver Domain	A domain that offers Service Enablers provided by a Donor Domain.
Donor Framework	An (OSA) Framework in the Donor Domain.
Receiver Framework	An (OSA) Framework in the Receiver Domain.
Donor Service	A Service Enabler provided by a Donor Domain that is offered by a Receiver Domain as if it where a Service Enabler in the Receiver Domain.
Receiver Application	An application that uses a Donor Service from the Receiver Domain.
Federation Service Profile	A Service Profile that serves as a template contract for a possible Agreement between the Receiver Domain and the Donor Domain regarding the use of a specific Donor Service.
Federation Service Agreement	A signed agreement between the Receiver Domain and the donor domain regarding the use of a Service Enabler.
Receiver Application Service Agreement	An agreement that allows a Receiver Application to use a specific Donor Service.
Service Enabler	An entity that offers Capabilities that can be used to construct and provide end-user services.
Proxy	An entity that provides services on behalf of another entity, by mimicking the entity that it is representing. Thereby possibly adding some pre- and/or post- processing.
Assertion	A statement by an Assertion Authority about authentication, authorization or attributes. An Assertion is typically an XML document. Assertions can be copied and handed over to other parties.
Assertion Authority	An Assertion Authority hands out Assertions. The Assertion can be signed and/or encrypted by the Assertion Authority.
Hand out/Hand over an Assertion	An Assertion is initially handed out by the Assertion Authority to the Assertion requestor. When the requestor has received the Assertion it can hand over (forward) the Assertion to another party.
OSA	Open Service Access - this abbreviation represents the concept of having standardized interfaces towards services and is practiced by Parlay (www.parlay.org) , 3GPP (www.3gpp.org) and ETSI (www.etsi.org)
OMA	Open Mobile Alliance – a telecom and IT industry Standardization initiative to enable services to mobile end-users.
Capability	A function that an operator domain can offer to other domains.